CS361 Questions: Week 13

These questions relate to Modules 16. Type your answers and submit them on Canvas.

Lecture 71

1. Explain the difference between the consumer and producer problems. Which do you think would be more prevalent?
2. Explain syn flooding.
3. Why are the first three solutions to syn flooding not ideal?

Lecture 72

1. How well does packet filtering work to prevent attacks?
2. What are the differences between intrusion detection and intrusion prevention systems?
3. Explain the four different solutions mentioned to DDoS attacks.

Lecture 73

1. Explain false positive and false negatives. Which is worse?
2. Explain what “accurate” and “precise” mean in the IDS context.
3. Explain the statement: “It’s easy to build an IDS that is either accurate or precise?
4. What is the base rate fallacy? Why is it relevant to an IDS?

Lecture 74

1. What did Code Red version 1 attempt to do?
2. Why was Code Red version 1 ineffective?
3. What does it mean to say that a worm is “memory resident”? What are the implications.

4. Why was Code Red version 2 much more effective than version 1?

Lecture 75

1. How was Code Red II related to Code Red (versions 1 and 2)?
2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
3. What did Code Red II attempt to do?
4. Comment on the implications of a large population of unpatched machines.
5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?