CIS 4930: Secure Coding [Fall 2018]
Test V

NAME: _____

Instructions:

1) This test is 5 pages in length.

2) You have 40 minutes to complete and turn in this test.

3) Short answer and essay questions include a guideline for how many sentences to write. Respond in complete English sentences. Responses will be graded as described on the syllabus.

4) This test is closed books, notes, papers, friends, neighbors, etc.

5) Use the backs of pages in this test packet for scratch work. If you write more than a final answer in the area next to a question, circle your final answer.

1. [20 points] [Essay]
Compare and contrast TCP and UDP. State advantages, disadvantages, and applications of each.

2. [25 points] [Essay]
For each layer in the OSI model, write 1 sentence to summarize that layer's purpose. In addition, for each of the 3 layers that introduce a new, standard kind of address in its headers, write another sentence to summarize the purpose of those addresses and provide a standard example, or class of examples, of such addresses.

3. [15 points]
a) Draw the 3-way handshake for establishing TCP connections (as we did in class).

b) Describe SYN-flood attacks; how and why do they work? [2-3 sentences]

c) Describe SYN cookies. [1-3 sentences]

4. [15 points]
In class we discussed DoS attacks in which attackers spoof IP source addresses and have third-party machines send, for example, error messages, to victims. What would an attacker look for in a protocol with a third party, to maximize such attacks? In other words, what would make one communication protocol "better" for an attacker than another?

5. [7 points]
Compare and contrast firewall and IDS policies. [2-4 sentences]

6. [7 points]
How do type-safe programming languages prevent attacks? What are 3 examples of attacks possible in C that are mitigated by type-safe programming languages? [2 sentences]

7. [6 points]
Why do dynamically typed programming languages tend to be type safe? [1-2 sentences]

8. [5 points]
What is the main difference between Mandatory and Discretionary Access Control? [1 sentence]