CNT 4419: Secure Coding [Fall 2022]
Test VI

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 guidelines for how much to write. Respond in complete English sentences. Responses will be graded as described on the syllabus. Additionally, do not use bullet points in your responses.

4) This test is closed books, notes, papers, smartphones, laptops, 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. [5 points] What are bandwidth-amplification attacks? [1-2 sentences]

2. [8 points] What are CSRFs, and how can they be mitigated? [2-4 sentences]

3. [5 points] At which OSI layer(s) do routers operate? [1 sentence]

4. [5 points] How and why do SYN cookies work? [1-3 sentences]

5. [3 points] What are three example web-application frameworks? [1 sentence]

6. [6 points] What is a CSPRNG? What is a CSPRNG intended to provide? [1-3 sentences]

7. [8 points] [Short essay] Compare and contrast session hijacking and fixation attacks.

8. [10 points] [Short essay] What does each layer of the OSI model do? Include information about layer numbers and addresses.

9. [25 points] Consider the following C code. Assume a 64-bit architecture, that all needed #include directives are present, that each character is stored in 1 byte and each integer in 8 bytes, that memory is laid out as in class (optimized to avoid a separate frame for printf), and that ca is user supplied, is heap allocated, has a 256 max size, and cannot be overflowed.

```
1       int f(char *ca) {
2           char str[512];
3           printf(ca);
4           gets(str);
5           return 0;
6       }
```

Assuming the system is using NX bits, ASLR, and StackGuard with 8-byte canaries, describe how a user could attack this program. Describe the attack at the level of detail we described attacks in class, including drawing memory when appropriate. [1-2 paragraphs]

10. [25 points] To keep things simple for this problem, assume that the only action of interest (i.e., the only security-relevant action) is `read(0)`.

a) Prove or disprove:

A property G is the union of a safety property and a liveness property iff G is a liveness property.

b) Suppose we were given a "random", or "arbitrarily chosen", property G. How likely is it that G is not a liveness property? Explain, using ideas discussed in class.