CIS 4930: Secure Coding [Fall 2018]
Final Exam

NAME: _____

Instructions:

1) This test is 10 pages in length.

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

3) Short answer 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. [2 points]
What does it mean for software to be secure? [1 sentence]

2. [4 points]
What is Return Oriented Programming (ROP)? [2-3 sentences]

3. [8 points]
a) Briefly explain ASLR and its limitations. [2-4 sentences]

b) Briefly explain CFI and its limitations. [2-4 sentences]

4. [5 points]
What are sound, complete, and precise mechanisms? How do these types of mechanisms relate to false positives and negatives? [3 sentences]

5. [4 points]
Why do we separate policies from mechanisms? What is the relationship between policies and mechanisms? [2-3 sentences]

6. [5 points]
Briefly explain each layer in the TCP/IP model. [1 paragraph]

7. [13 points]
a) What does it mean for a set to be countable? [1 sentence]

b) Prove or disprove that 2^N (i.e., the set of all sets of natural numbers) is countable.

c) Referring to your solution to part (b), are policies countable? Explain your intuition and assume that the set of programs is countably infinite. [1-3 sentences]

8. [6 points]
In class we discussed ~8 types of SQLIAs, including, for example, timing attacks. Show 3 output programs (with injected inputs underlined) to illustrate 3 different types of SQLIAs.

9. [3 points]
Name 3 standard C-library functions that may be avoided to mitigate buffer overflows.

10. [11 points]
a) Explain the steps in a Diffie-Hellman key exchange. [1 paragraph]

b) Under what attack model does the D-H key exchange operate? [1-3 sentences]

c) How can an active attacker mount two different kinds of attacks on D-H? Explain in enough detail to convince a reader that the attacks work. [1 paragraph]

11. [8 points]
Consider the following code. Assume a 64-bit architecture, that all needed #include directives are present, that each integer is stored in 4 bytes, and that `input` is allocated on the heap.

```
1   int f(char *input) {
2     char a[8];
3     a[0] = 'a';
4     printf(input);
5     return 0;
6   }
```

a) Draw a representation of the program memory segments (including their contents when known) right before the `printf` is executed, at the level of detail shown in class. Assume an optimized layout of memory, as discussed in class, where `printf` is not given its own frame.

b) Assuming `input` is "n%p%p%n", describe what happens when running the `printf`, at the level of detail discussed in class.

12. [8 points]
Explain, using an example, how an integer-overflow attack may proceed. As part of your example, show the vulnerable code. [1 paragraph]

13. [12 points]
For all the following, respond at the level of formality presented in class.
a) Formally define properties.

b) Formally define safety properties.

c) Formally define liveness properties.

d) The formal definition of policies discussed in class could be called a qualitative model, because the definition qualifies some programs as "good". Other models consider policies quantitatively; these models quantify how good programs are (e.g., on a scale of zero to one). Formally define policies in a quantitative model.

14. [9 points]
a) What are the ideal properties of cryptographic hash functions? [1 paragraph]

b) What is a CSPRNG? [1 sentence]

c) Compare and contrast MACs and digital signatures. [2-4 sentences]

15. Dessert. [2 points]
What is a cookie (aka magic cookie)? [1 sentence]