CNT 4419: Secure Coding [Fall 2023]
Test III

NAME: _____

Instructions:

1) This test is 7 pages in length.

2) You have 75 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. Respond at the level of detail discussed in class. Avoid using bullet points and enumerated lists.

4) This test is closed books, notes, papers, phones, smartwatches, 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. [2 points] What is another name for the TCP/IP model?

2. [3 points] What are TOCTOUs? [1-2 sentences]

3. [5 points] How does CFI provide a foundation for runtime monitors? [2-4 sentences]

4. [6 points] Why does each layer in the TCP/IP model have the name it has? [Essay]

5. [15 points] For each of the following classes of attacks, write a short paragraph summarizing what application-level coders can do to mitigate those attacks.
a) Buffer-overflow attacks

b) Format-string attacks

c) Integer-overflow attacks

6. [6 points] [2-4 sentences]
We defined type safety in class both intuitively and more precisely (in terms of programming-language semantics). What are both of these definitions?

7. [10 points] [Essay]
Explain firewall policies and mechanisms. As part of your explanation, include an example firewall policy to help show how conflicts between rules are typically resolved.

8. [10 points] [Essay] In class we saw an example of an integer-overflow attack leading to an out-of-bounds write. Now show and briefly explain an example integer-overflow attack leading to an out-of-bounds read.

9. [10 points]
Consider a simple type-safe programming language L having two types, int and bool. Expressions in L can be integer or Boolean literals, addition expressions, or conditional expressions of the form "if e1 then e2 else e3", where e1, e2, and e3 are subexpressions. In a well-typed conditional expression, the "then" and "else" branches must have the same type. Conditional expressions evaluate by first figuring out which branch to execute and then executing the appropriate branch.

Define L's syntax and semantics, using the conventions discussed in class.

10. [17 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 4 bytes, and that the getStr function returns a user-entered string allocated on the heap.

```
1     void f(char *s) {
2       printf(s);
3       return;
4     }
5     void g(char *s) {
6       char st[32];
7       st[0] = '0';
8       f(s);
9       return;
10    }
11    int main(int argc, char *argv[]) {
12      g(getStr());
13      return 0;
14    }
```

a) Draw a representation of the program memory segments (including their contents when known) while the printf is executing, at the level of detail shown in class. Assume the system uses 4-byte stack canaries and an unoptimized layout of memory, as discussed in class, where printf is given its own frame. Also show SP and FP.

b) Assuming s is "000%d%d%d%n", describe what happens when running the printf, at the level of detail discussed in class. [1-2 sentences]

11. [16 points] Consider the following C code. Assume a 32-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 (unoptimized, with printf having a separate frame), and that b is user supplied, is heap allocated, has a max size of 32, and cannot be overflowed.

```
1     void a(char *b) {
2       char s[128];
3       printf(b);
4       gets(s);
5       return;
6     }
```

a) Assuming the system is using NX bits, ASLR, and 4-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]

b) Explain whether CFI would mitigate the attack you just described. [1-2 sentences]