CNT 4419: Secure Coding [Fall 2019]
Test 5

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. Avoid bullet points. Responses will be graded as described on the syllabus.

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. [15 points]
For each of the following acronyms discussed in class, expand (define) the acronym and briefly describe what the term refers to. [1-2 sentences each]

a) MAC

b) UDP

c) ICMP

d) TLS

e) OSI

2. [12 points] [Short essay]
Name and describe Layers 4 and 6 of the OSI model.

3. [12 points] [Short essay]
For the TCP/IP model, describe the new addresses introduced by each layer, if any. Be sure to specify the names and lengths of the addresses as they are used in practice.

4. [20 points]
a) Prove or disprove that the set of sets of natural numbers is countably infinite.

b) Referring to your solution to Part (a), are policies countable? Explain your intuition. [1-2 sentences]

5. [25 points]
Consider the following 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 4 bytes, and that the get_input function returns a user-entered string allocated on the heap with a max size of 512 characters and cannot be overflowed.

```
1       int f(char *input) {
2           …
3       }
4       int main(int argc, char *argv[])
5           f(get_input());
6           return 0;
7       }
```

a) Without using the gets function, write the body of f such that it is vulnerable to a buffer overflow attack. Assume NX bits, ASLR, and StackGuard are not implemented.

b) Describe the attack at the level of detail we described attacks in class, including drawing memory when appropriate. [1 paragraph]

c) List three techniques (besides NX bits, ASLR, and StackGuard) discussed in class that could prevent your attack from Part (b).

6. [16 points]
Explain, using an example, how an integer-overflow attack may proceed. As part of your example, show the vulnerable code. [1-2 paragraphs]