CNT 4419, Sec 001, Test 3, 75 minutes **NAME:**_____

Instructions: All the instructions that are on the syllabus. For example, this test is closed everything, including phones, notes, AI, and other students. Do not talk to another student during the test. Do not look at another student's answers during the test. Do not ask a question during the test that gives away any part of any answer. If a response length is indicated, respond at that length and do not use bullet points or enumerated lists. Unless stated otherwise, use the same notations, definitions, and assumptions that we have been using in class. Respond at the level of detail discussed in class. This test is 5 pages.

1. [6 points] As discussed in class, what are standard techniques for mitigating insider threats? [1 sentence]

2. [5 points] Compare and contrast session fixation and session hijacking attacks, hitting all the main points discussed in class. [2 sentences]

3. [4 points] What does it mean for mechanisms to be sound or complete? Regarding soundness and completeness, what does one generally aim for, in practice? [1-3 sentences]

4. [10 points] Consider the Employees table shown below.

EID	**Name**	**Salary**
1	Alice	10.2
2	Bob	22
3	Eve	35

a) Define a logical schema for the Employees table.

b) Write a SQL statement to define (but not populate) the Employees table.

c) Write a SQL statement to populate the first row in the Employees table.

d) Write a SQL statement to add a new column to the table, to store each employee's address.

e) What does this SQL statement do? UPDATE Employees SET salary=salary*1.025 [1 sentence]

f) Write a SQL statement to delete the Employees table.

5. [8 points] Show and explain (in 2-3 sentences) an example of a standard firewall policy, including how conflicts get resolved, as discussed in class.

6. [4 points] Name, and summarize the functionalities of, OSI Layers 5 and 6, hitting all the main points discussed in class. [2 sentences]

7. [5 points] What is/are the instructor's argument(s) that location should not be considered a fourth authentication factor? Hit all the main points discussed in class. [1-3 sentences]

8. [8 points] Suppose that a thief obtains the password to unlock a victim's phone, steals the phone, and successfully uses the password on the stolen phone.
a) Explain how the phone's password checker may be considered to exhibit a false negative. [1-2 sentences]

b) Explain how the phone's password checker may be considered to exhibit a true negative. [1-2 sentences]

9. [6 points] What are all the different network addresses we discussed in class as being widely used in practice, and what is the size of each? [1 sentence]

10. [6 points] Recall the echo program from class and call it p_{echo}. We identified p_{echo}'s traces in class. Now consider $P = \{p_{echo}\}$ and prove where P lies in our map of policies. In other words, prove whether P is a property, safety, and/or liveness.

11. [12 points] Prove the assertion from class, that G_{all} is the *only* property that's both safety and liveness.

12. [26 points] [Essay] Consider the following C code. Assume a 16-bit architecture, that all needed #include directives are present, that each character is stored in 1 byte and each integer in 4 bytes, that memory is laid out as in class (optimized to avoid a separate frame for printf), and that str is user supplied, is heap allocated, has a 180 max size, and cannot be overflowed.

```
1       int fun(char *str) {
2           char ca[256];
3           printf(str);
4           gets(ca);
5           return 0;
6       }
```

Assuming the system is using NX bits, ASLR, and StackGuard with 2-byte canaries, describe how a user could maximally attack this function. Describe the attack at the level of detail we described attacks in class, including providing attack input(s) and drawing memory when appropriate.