CNT 4419 Quiz 4/2/25 (20 minutes) NAME: _____

Instructions: Consider the following C code, which contains a security vulnerability. Assume that all required #includes are present; the program is valid and executed on a 64-bit architecture; none of the library functions return errors during execution; all mallocs get allocated into contiguous (adjacent) memory, each allocation immediately after the previous one, with earlier mallocs at lower addresses than later mallocs; and there are no extra security mechanisms in place (no NX bits, canaries, ASLR, or CFI).

```
#define LEN 32
typedef struct security_flags {
  char disallowFileAccess; //if nonzero then disallow access to file system
  ... //etc.
} SF;  //now the type SF refers to a record of security flags for the program
void setup_flags(SF *sf) { //implement a secure default: disallow everything
  sf->disallowFileAccess = 1;
  ... //etc.
}
int str_len(int base, char need_nul) {
  if(need_nul) return base+1; //add 1 extra byte if a NUL-terminator is needed
  else return base;
}
int main() { //Reminder: the argument to malloc is the # of bytes to allocate
  char *s = (char *)malloc(LEN);
  SF *sf = (SF *)malloc(sizeof(SF));
  setup_flags(sf);
  fgets(s, str_len(LEN,1), stdin);
  ... //etc.
}
```

Here is documentation for the function "`char *fgets(char *s, int n, FILE *stream)`":
The fgets() function shall read bytes from stream into the array pointed to by s until n-1 bytes are read, or a <newline> is read and transferred to s, or an end-of-file condition is encountered. A null byte (i.e., a byte of 0s for the NUL-terminator) shall be written immediately after the last byte read into the array.

1. [5 points] Explain the vulnerability and a possible attack. Be sure to use terminology discussed in class and categorize the vulnerability as completely as possible. [Short essay, may continue onto next page]

2. [1 point] Would NX bits mitigate the code vulnerability? Explain. [1 sentence]

3. [1 point] Would stack canaries mitigate the code vulnerability? Explain. [1 sentence]

4. [1 point] Would ASLR mitigate the code vulnerability? Explain. [1 sentence]

5. [1 point] Would CFI mitigate the code vulnerability? Explain. [1 sentence]

6. [1 point] What are 2 **logically distinct** code modifications/rewrites that a programmer could implement, to mitigate the vulnerability? [1 sentence]