Sample Midterm Exam

1. Here is a fragment of code from a program that reads data from a file into a dynamically allocated part of memory. There are at least 3 things in this code that make it very non-robust. Find any 3, say why each is a (potential) problem, and how you would fix each. (This question asks about robustness, not commenting style – the comments are just there to help you figure out what is going on.)

```
/* read nchars characters from the file named filename */
/* and put them into dynamically allocated memory      */
char *load(int nchars, char *filename)
{
      char *p;    /* pointer to allocated memory */
      FILE *fp;   /* pointer to the opened file */

      /* allocate space for nchars char */
      p = malloc(nchars * sizeof(char));
      /* open the file */
      fp = fopen(filename, "r");
      /* read nchars characters from the file that   */
      /* fp points to, and put it in the memory that */
      /* begins at address p                         */
      (void) fread(p, sizeof(char), nchars, fp);
      /* close the file */
      (void) fclose(fp);
      /* return the address of the allocated memory */
      return(p);
}
```

2. Why is a precise statement of security requirements critical to the determination of whether a given system is secure?
3. Please describe how the vulnerabilities models are used during the Flaw Hypothesis Methodology. Be explicit: which phase of the methodology uses them, and how?
4. Into which category or categories of the Program Analysis classification do the following fall? Please justify your answer.
   a. Buffer overflow causing a return into the stack?
   b. Allowing an ordinary user to alter the password file?
   c. Simultaneous writes to a shared database?
   d. Reading a UNIX file by directly accessing the raw device and reading first the superblock, then the file’s inode, and finally the file’s data blocks?
5. Consider the Bell-LaPadula multilevel security model. If a subject with security label (*L*, *C*) can read an object with security label (*L’*, *C’*), then (*L*, *C*) is said to *dominate* (*L’*, *C’*). Prove that this *dominates* relation is reflexive, antisymmetric, and transitive.