MITS 5400G - Assignment 1

*Compile your answers to the following questions (including any C code, screenshots, and drawings) into a **single PDF** file and submit it online.*

1. [2 point] Compare and contrast Waterfall vs Scrum software process models.
2. [2 point] What is Test Driven Development (TDD) software development process? And how is it different than software testing in the Spiral software process model?
3. [2 point] Which one of the fundamental security design principles is being violated in the following code? How do you propose to fix it?

```
01      int main(){
...             ....
10              DWORD dwRet = IsAccessAllowed(...);
11              if (dwRet == ERROR_ACCESS_DENIED){
12                      //Security Check failed.
13                      // Inform user that access is denied
14              } else {
15                      //Security check is OK.
16              }
17
...             ....
101             return 0;
102     }
```

4. [6 points] We have utilized the Microsoft Threat Modeling Tool to assess potential threats against our proposed IoT Blood Pressure Monitoring System, as detailed in the file available on our course's Canvas page. The software has identified **six threats** impacting "Availability." For each threat, provide a description of the details highlighted by the software, along with your proposed solutions to mitigate these threats.

   Note: use View>Analysis View, then View > Threat List, and View > Threat Properties to activate relevant panels.

5. [6 points] Create an attack tree for reading someone else's OntarioTechU emails using ADTree tool.
   a. Assign a probability of success to each attack leaf node, providing a rationale for each value assigned. You may base your argument on personal judgment or an online source. However, bear in mind that using personal judgment as a basis may necessitate a more robust justification compared to relying on information from an online source.
   b. Add defense nodes to your attack tree and determine the probability of their effectiveness, that is, their likelihood of success. For each assigned value, provide a supporting argument. You may base these on your own judgment or refer to an online source. However, keep in mind that relying on personal judgment might require more substantial justification than using information from an online source.

Note1: take a screenshot for your attack tree after step 5.b. Make sure the nodes are readable. Add the screenshot to your document.

Note2: Your tree will be graded based on its completeness and soundness of defensive measures.

Note3: You can download "ADTool-1.4-jar-with-dependencies" from the assignment page. But you have to make sure that Java Runtime Environment (JRE) is installed on your device in order to run the application.

6. [5 points] Carefully study the given Rock-Paper-Scissor program source code. (`rockpapersicssor.c` can be found under Assignments>Assignment1 on Course Canvas.)

   a. There is one (at least) buffer overflow vulnerability in the code that can help you to "always" win over the computer! Describe the vulnerability, draw the details of the affected stack frame, precisely illustrate the relative locations of the local variables on the stack, and how/which variables are affected by the buffer overflow vulnerability.
   b. Capture a screenshot clearly demonstrating the successful exploitation of the buffer overflow vulnerability (showing you have won consistently against the computer and the inputs you have entered).
   c. How do you propose to fix the buffer overflow vulnerability you discovered in 6.a ? (Provide the required C code.)

   Note1: You are expected to compile this code on virtualized Kali Linux environment.