NAME: **ALPHA:**

SY485J: Lab 4: Lives may depend on you solving this

Go to http://courses.cyber.usna.edu/~debels/SY485J/Code/Lab4. You are an intern at NSA and it is your second day in your office. Your office is responsible for evaluating the cryptographic implementations of network security products from different targets. Due to you telling your boss that you had taken a Software Reverse Engineering course, you are asked to work on a time sensitive project that has just come in. Due to lack of personnel in the office due to budget cuts, you must work on this project alone, as everyone else has other projects. You are only given one file: random.exe. random.exe is an executable file. You can execute it. You are told that the fils was "acquired" by an HUMINT asset and it is believed that the executable is from a high value target's computer, meaning we want as much intelligence on this target as possible. Your boss tasks you with discovering what this executable is doing. Answer the following questions about the file and in the process you will be helping your office understand more about this target. In addition to exe, you have access to objdump and gdb (no other dynamic analysis tools are available in this office), and the Internet for search purposes. Due to time sensitivity, because this high value target will be coming to the U.S. on Saturday September 21, 2019 your boss needs answers to these questions no later than, 1055 Friday, September 20.

1. (10 points) How many command line arguments (to include options) are expected when you run the program? For example, "random.exe –x file1 file2" would be 4 arguments.

2. (25 points) List each command line argument (including the name of the executable) and provide a brief (one sentence) but specific description as to what each represents.

NAME: **ALPHA:**

3. (15 points) Looking at the static code, list 3 things in the assembly that provide you with hints as to what the code is doing.

4. (10 points) Name one function that is not called when this code is run. What do you think this function is doing? Why do you think it’s not being called?

5. (20 points) When you execute the code, what are the first three functions (not including main()) called? What, in layman’s terms, is the purpose of these three functions?

NAME: **ALPHA:**

6. (20 points) What, overall, is “random.exe” doing? Is it performing the function of a “product”, like a VPN, firewall, or something else? Explain, in layman’s terms using as much detail as possible. Don’t leave out any steps.