Project 2

Program 2

Andrew Beers acb75@pitt.edu

Procedure:

Knowing the program was written in C, I knew it would have a main function. I initially set a breakpoint at main. After disassembling main I saw that it wasn’t too much of help to me, but I saw it was calling a new function d, so I set a breakpoint for d. After disassembling d, still no nice strcmp functions to find but I found other functions c and e, so I set break points at both of those as well. I reran the function disassembling at functions c d and e and saw there was a new function s being called in both c and e. I set s as break point as well. After inspecting the assembly code I made the assumption that d was almost acting as the main function in this program. With this in mind I attempted to see what the other functions in the program were doing. I found that s seemed to be a single character comparison version of strcmp, while c and e were doing all of the book keeping of indices. I noticed in the beginning of c that there was an initialization and a test at the beginning to skip to the end of c, I assumed this initialization to be the import of the pass code from the string table. I did a breakpoint at this point in the program (0x080484b7) and tested the value in $ebx.

Solution:

The value I received from the set breakpoint was “3.141593”. I reran the program with this input and the passcode was unlocked.

Notes:

This program differed from the first in a way that you had to set breakpoints to functions other than main and follow the flow of the program. This program had many more function calls than the program in part 1 and because of this took much longer to crack the passcode.

Pass phrase-3.141593