Project 2 Write Up
Nick Miller
CS 449

Program: nam99_1
Password: wEMACsFzmGtlZkGpteQo
Process: The process of getting the password for nam99_1 was fairly simple. After successfully creating a mystrings program, my first instinct was to just search the program for the words “pass” or “phrase”. After I did this I got a result that said “Unlocked with passphrase %s”, and then before this and before “Sorry! Not correct” there was a long string of characters. And I thought maybe that could be the passphrase, so I copied the passphrase, reran the program and then pasted it as the answer and got the correct answer.

Program: nam99_2
Password: A palindrome. (“helloolleh”)
Process: This was a little trickier then the first one. I first started by doing objdump with the program and dumped it into a text file so I could read through it. I found out that there are functions that do different things, so like function s counts the number of chars. I also realized that before <s> is called the ‘\n’ character is removed. So I set breakpoints at s, c and p. Then once I hit these breakpoints I used the stepi command to go through the code. Though this helped me figure out the length of the string had to be 8 or greater, it was still difficult to decipher what was going on. So I tried with trial and error trying to figure out the word so I tried “aaaaaaaa” and it worked. So I tried “aaaaaaab” and “baaaaaaa” and no luck. So then I got to thinking about the palindrome mentioned in class, so I tried “HelloolleH” and it worked to, and I kept trying different lengths and it worked every time.

Program: nam99_3
Password: Unknown
Should be Password: The password should be any combination of 10 characters that has 6 characters that there ASCII value minus 65 is less than 4. So hypothetically “!!!!!!abcd” should word
Process: Now this was a doozy of a code to try and unscramble. The first thing I tried was to simply run the GDB and try and see if I could get something out of it. But I couldn’t. So I used objdump -d, and printed that out to a text file so I could scroll through it easily. I deciphered the code, and once I got passed instruction 0x804845b I started to actually see a program. I was able to figure out the program checked for 9 or more characters and initialized a array (and a few other simple initializations), and then went into a while loop. In this while loop it ran if cnt was less than 10, and cnt was set to 1 originally. So in this while loop there were 2 variable initializations right off the top which was one that I called startVal which was equal to cnt minus 1 and lower which was equal to tolower(*(input_str+index)). Then it checked if lower - 65 was greater than 4 and if so just cnt was incremented. If not, cnt and cnt2 were incremented. After the while loop was over then if cnt2 was equal to 6 you got congratulations, if not you didn’t. So I thought I figured out what it needed to be but no combination was still working. There was a weird process in the actual code, and this one proved to be not possible. So I put break statements where cnt2 would increment and this statement was never reached, and I tried every combination of letters repetitively (e.g “aaaaaaaaaaa”, “!!!!!!!!!!!”, …). So I deduced getting inside of this if loop, where cnt2 was incremented is not possible. I think you can not get into this loop

because of a bug in the tolower function. Also then I got an email from professor which was a sigh of relief.