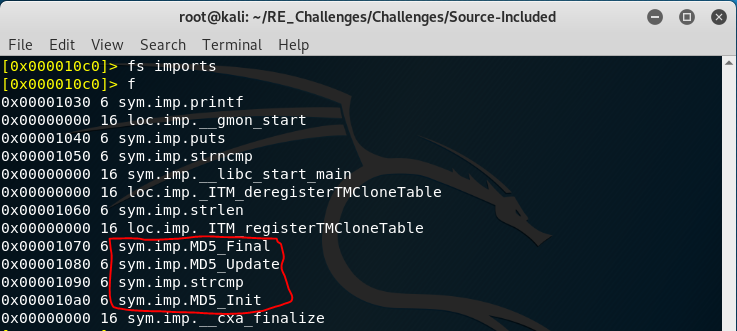
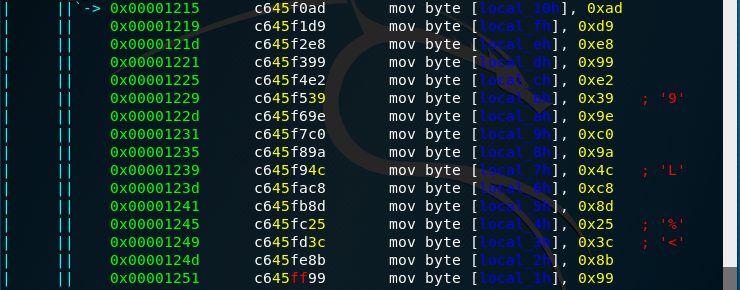
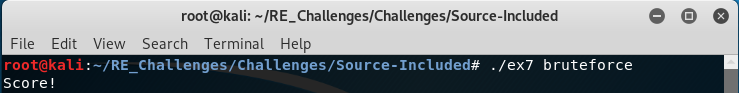
***Ex7***

This one could possible ruin your day, week maybe even month if you let it. It is actually pretty simple if you know the details of what is being used inside the program. Lets start off by seeing what some of the functions in the program will be.

If you read the help for ex0 then you remember flag spaces. Let’s takes a look at the imports flag space to see what functions are imported into the program. We see some functions prefixed with MD5\_, these are the functions needed to calculate a MD5 hash, message digest 5. MD5 was designed in 1991 and is a well-known hashing algorithm that is rather fast. It is not used much anymore at least for cryptography for this exact reason, speed. To those that are not aware a hashing algorithm is a one-way function, as in it has no inverse function to apply to the functions result to get the original input. This may seem impossible to reverse and it literally is BUT, with how fast the algorithm is designed to be we can quickly calculate a large amount of hashes until we find one to match the hash we have and we will know what the original input used to generate the hash in question was. For our more math-oriented people this is known as a “pre-image” attack, since the input of a function/mapping is called the pre-image. Now lets see if we can grab this hash to start brute forcing it.

As you would expect finding the hash is obvious especially if you know that an MD5 hash is 128 bits or 16 bytes long. Here we have all 16 bytes in order! How will we bruteforce it though?

There are MANY databases online of known MD5 hashes and their associated pre-image values. Find one, throw it our hash and wait, usually the amount of time it takes to refresh your page then Score!

If you feel adventurous you could look into using the tools called “hashcat” and “crunch” to solve this challenge. Hashcat is a hash cracking program that can be set up to either use your cpu or gpu to compute a list of values with many hashing algorithms and check the results with a list of hashes. Crunch is a text generating program that can be used to “pipe” its output to hashcat so you do not have to generate a large text file and have it stored on disk, they can quickly reach into sizes that you can not store on your computer if you are not careful.