STEP 1: Problem definition

this program executes some bash functions.

the user inserts a message (the command) and if

the command is contained in a list of 'executable'

commands, it executes it.

From the if-else block defined in the main,

we can notice that the only command allowed

is ls.

As usual, we need to define a possible entry point,

which is the 'gets' defined on line 17. This fills the

variable buffer (line 14) of 32 bytes.

what can we do next? the target is to execute denied commands

such as 'cat flag.txt'

what is the function 'lol'? (line 9)

it contains \_\_asm\_\_, which allows us to include and execute

assembly instructions. In this case, it jumps to the address

contained in %esp (so the program is using the x32 architecture)

ESP is the stack pointer