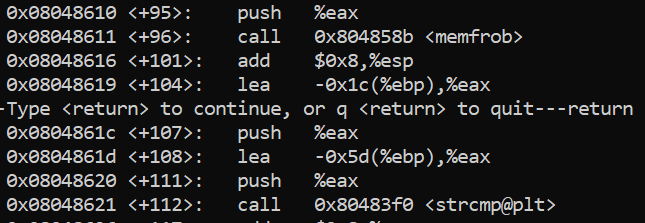
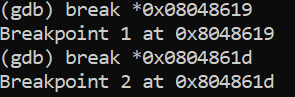
Pass : aesebootiv

Step 1: disassembly main function behemoth0 using GDB

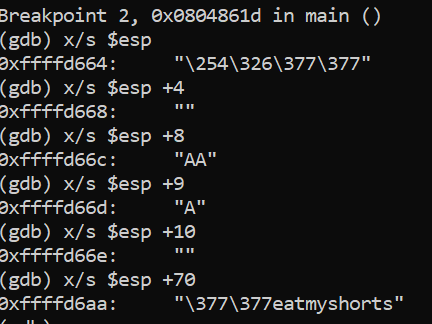


We can see that there is strcmp function that load the real password from another location and before we call strcmp we load to the stack the passwords in 0x08048618 and 0x0804861d.

Step 2: create breakpoint



Step 3: run and display text using x/s $esp



The pass word for behemoth0 is "eatmyshorts"

Behemoth0 run as behemoth1 so we can output the next password.

