Bomba de Manuel Guerrero Mesías

Pasos por orden(solo tendrás que abrir el terminal en la carpeta donde este la bomba.c y poner cada una de las siguientes lineas, cada linea va seguida de un enter. Si en algún momento en la pantalla se mezcla la informacion podemos reorganizarla pulsando control+l):

gcc -Og bomba.c -o bomba -no-pie -fno-guess-branch-probability
gdb -tui bomba
layout asm
layout reg
br main
run
nexti*16 (hasta que nos pida la constraseña donde introduciremos lo que queramos)
nexti*3
stepi (para entrar en la función masageador)
nexti*3
set $eax=4 (para saltarnos el bucle for donde no se hace nada interesante)
nexti*2 (Aquí descubrimos que a la contraseña que le hemos pasado a la función, que es la que nosotros hemos introducido, se le suma a la posición 9 la cantidad de 32 esto pasado a lenguaje ASCCI y sin dar muchos rodeos es lo mismo que pasar de una letra mayúscula a la misma letra pero minúscula. Esto lo confirmamos haciendo la instrucción p(char*)$rdi con la cual vemos que la variable $rdi contiene nuestra contraseña)
step (como ya hemos averiguado lo que hace con la contraseña alfanumérica ya podemos salir de la funcion con la orden step)
nexti*5 (aquí encontraremos la contraseña autentica así que lo único que tenemos que hacer para averiguar cual es nuestra contraseña es meter la que pone pero la letra en la posición 9 ponerla mayuscula es decir la ‘s’)
nexti*2
set $eax=0
nexti*6
set $eax=0 (para saltarnos la comprobación del tiempo tarda)
nexti*10 (introduciremos un pin del que nos acordaremos)
nexti*6
stepi (entramos en la función para nada sospechosa para ver que hace)
(Ahora en la instrucción lea vemos que en la variable rdi esta el código que hemos introducido, como ya todos “sabemos” lo que pasa en esa linea es lo siguiente: sumar el numero con siguo mismo y guardarlo en eax para su devolución).
nexti*3 (Ahora vemos con la instrucción p*(int*)0x601064 vemos el código ahora ya sabemos todo lo que hay que introducir para pasar la bomba: contraseña: locopizzaS y código: 4444).