

## 1 Uso de gdb

Utilicé el debugger de GNU para obtener las instrucciones de ensamblador del binario `help_me`. Los comandos :

- `$ gdb help_me`
- `(gdb) start`
- `(gdb) disass main`

```
Starting program: /home/dmontes/basura/elege/Ejer/dia3/help_me
ssssss
reprobado
[Inferior 1 (process 12019) exited with code 012]
(gdb) start
Punto de interrupción temporal 1 at 0x8048489
Starting program: /home/dmontes/basura/elege/Ejer/dia3/help_me

Temporary breakpoint 1, 0x8048489 in main ()
(gdb) disass main
Dump of assembler code for function main:
```

Figure 1: Inicio de gdb.

Encontre *el pan*. La función para comparar cadenas. Seguro esa era la que me iba a dar la cadena que buscaba En la página <http://www.debasish>.

```
.../bin/03020-~/basura/elege .../bin/03020-~/basura/proy .../~/basura/elege/Ejer/dia3
0x080484e0 <+101>: call    0x8048370 <__isoc99_scanf@plt>
0x080484e5 <+106>: add     $0x10,%esp
0x080484e8 <+109>: sub     $0x8,%esp
0x080484eb <+112>: lea     -0x8b(%ebp),%eax
0x080484f1 <+118>: push    %eax
---Type <return> to continue, or q <return> to quit---
0x080484f2 <+119>: push    $0x80485c7
0x080484f7 <+124>: call    0x8048330 <strcmp@plt>
0x080484fc <+129>: add     $0x10,%esp
0x080484ff <+132>: test    %eax,%eax
0x08048501 <+134>: jne     0x8048515 <main+154>
```

Figure 2: Comparación de cadenas

in/2012/01/reversing-simple-program-with-gdb.html encontré un comando de gdb para imprimir dada una dirección

```
(gdb) print
print      print-object printf
(gdb) printf "%s\n" 0x80485c7
Sintaxis de argumento inválida
(gdb) printf "%s\n" $0x80485c7
Sintaxis de argumento inválida
(gdb) printf "%s\n", $0x80485c7
El valor no se puede convertir a entero
(gdb) printf "%s\n", 0x80485c7
hola :)
(gdb) █
```

Figure 3: Impresión de la cadena con la que se compara la entrada