Práctica 4: Desactivación de Bombas

Desactivación Bomba de Álvaro Luna

Pablo Olivares Martínez

`contraseña = "holahola"`

`pin = 4321`

Para comenzar, ejecutaremos ltrace para ver con qué string compara nuestra cadena introducida. Vemos que compara con ***holahola***, así que como no parece tener ninguna modificación, probemos si es ésta la contraseña.

```
pablo@laptop:~/Bombas$ ltrace -i -S ./ALR_bomba2020

                                                ...

[0x7f155600f1e7] SYS_write(1, "Introduzca la contrasenia: ", 27Introduzca la
contrasenia: ) = 27
[0x7f155600f142] SYS_read(0holahola
, "holahola\n", 1024) = 10
[0x4007b1] <... fgets resumed> "holahola\n", 100, 0x7f15560e9980) =
0x7fffbac81190
[0x4007cc] strncmp("holahola\n", "holahola\n", 10) = 0
```

Efectivamente, el valor es correcto. Ahora veamos cuál es el código. Para ello abramos gdb y analicemos el código. Vemos que hay varios identificadores, pero veremos que el que nos interesa es: **# 0x601060 <adios>**. Vemos que hay varias variables declaradas para despistar, sin embargo, analizando un poco el código vemos la siguiente comprobación:

```
|   0x40085f <main+260>     mov    0x2007fb(%rip),%eax        # 0x601060
<adios>          |
|   0x400865 <main+266>     cmp    %eax,0xc(%rsp)
          |
|   0x400869 <main+270>     je     0x400870 <main+277>
           |
|   0x40086b <main+272>     callq  0x400727 <boom>
  |
```

Aquí vemos que el código compara <adios> con el valor introducido y si coinciden, se salta el boom. Por tanto, podríamos sospechar que el código fuese adios. Para ver los valores de <adios>, podemos poner un breakpoint en main+266 y ver los valores que compara:

```
br *main+266
p $eax
$1 = 4321
```

Como vemos que no hay ninguna modificación del valor introducido, deducimos que el **código** es **4321**. Por tanto, introducimos los valores en la bomba y vemos que funciona:

pablo@laptop: ~/Escritorio/Bombas

```
pablo@laptop:~/Escritorio/Bombas$ ./ALR_bomba2020

Introduce la contrasenia: holahola

Introduce el pin: 4321

Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·
Â·Â·Â· bomba desactivada Â·Â·Â·
Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·Â·
```