Documentación
PRÁCTICA 4

Estructura de computadores

UNIVERSIDAD
DE GRANADA

Fernández Mertanen, Jonathan

Resolución de mi bomba

Password

La primera llamada a encrypt tiene de argumentos r:vk y 10

- En $r8 se almacenan los cambios en cada iteración: r:vk -> h:vk -> h0vk -> h0lk -> h0la

La segunda llamada a encrypt tiene de argumentos lo que hemos introducido y 10

- Sigue el mismo bucle

Deducimos que decrementa cada carácter en 10, menos el segundo.

```
0x4007fc <main+107>     subb   $0x3f,0x3b(%rsp)
0x400801 <main+112>     subb   $0x3f,0x41(%rsp)
```

Estas instrucciones restan 63 a los segundos caracteres de ambas cadenas, por lo que al segundo carácter en vez de añadirle 10 se le eliminan 73 (63+10)

La contraseña es: ryvk que encriptada es h0la

Code

```
<main+286>      mov    0x2007ab(%rip),%eax        # 0x601060 <token>
<main+292>      mov    0xc(%rsp),%edx
<main+296>      sub    %eax,%edx
<main+298>      add    $0x46a2a,%eax
<main+303>      cmp    %eax,%edx
```

token = 2 = eax
??? = edx
edx - token
289322 + token

compara edx-token y 289324

edx debe ser el número que hemos introducido, ya que la otra parte de la comparación no tiene nada que ver
Por lo que el pin es 289326 (introducido-token = 289324)

Solución

PASSWORD: ryvk
PIN: 289326