Bomba de Alejandro Rubio Martinez

Contraseña: movimientohelicoidal

PIN: 1001

La dificultad de esta bomba está en su simpleza. Mientras que a lo largo del main podemos observar multitud de operaciones que se realizan a la contraseña y el pin, las cuales están declaradas con nombre confusos (la constraseña se llama nomemires y el pin como password), pero que si observamos vemos como tan solo son operaciones inútiles. Por ejemplo:

```
0x401257 <main+141>     call   0x401050 <strlen@plt>
0x40125c <main+146>     imul   $0x32,%eax,%eax
0x40125f <main+149>     add    $0x1,%eax
```

Vemos como lo que tenemos en %eax, que es el pin de la bomba lo calculamos como el número de letras de una frase (la contraseña) multiplicado por 50 y sumándole uno, pero podemos pasar estas operaciones y luego observar tan solo el resultado final.

Para ello vamos a buscar instrucciones que comparen cosas en nuestro código. Si bajamos atentamente llegamos a:

```
   0x4012b1 <main+231>             cmp    %eax,0xc(%rsp)
   0x4012b5 <main+235>             jne    0x4012d1 <main+263>
   0x4012b7 <main+237>             lea    0x30(%rsp),%rdi
   0x4012bc <main+242>             mov    $0x15,%edx
   0x4012c1 <main+247>             lea    0x2da8(%rip),%rsi
   0x4012c8 <main+254>             call   0x401030 <strncmp@plt>
```

En main+235 haciendo `p(int)$eax` obtenemos el pin que es 1001;

En main+254 haciendo `p(char*)$rsi` obtenemos la contraseña que es "movimientohelicoidal".

Entonces la forma más rápida de hallar los datos de mi bomba sería:

```
#Esto sería un archivo .gdb
file bomba_ARM_2020
#Ahora establecemos un punto de ruptura en la linea que queremos
br *main+231
#Veamos el valor del pin
p(int)$eax
#Bajemos hasta donde podamos ver la contraseña
ni
#Ahora si quisiéramos cambiar la contraseña para que coincida con la que hemos
introducido, por ejemplo, si introducimos de contraseña enchufe
set $eax="enchufe"
#Seguimos bajando
ni
ni
ni
ni
#Ahora veamos el PIN
p(char*)$rsi
```

```
#Ahora para cambiar el pin, suponiendo que hemos introducido el 777
ni
set $rsi=777
```