

Pratica 4: Bombas resueltas

- Bomba María Alcázar Marcos

Contraseña:Rorrecta

Pincode:7777

```
Actividades - Terminal - Vie 20:17
juse@juse-OMEN-by-HP-Laptop: ~/Escritorio/Universidad_ubuntu/EC/Practica4/Bombas_resueltas/Maria_Alcazar_Marcos

--Register group: general
rax      0xffffffffc30 140737488346160  rbx      0x0 0
rsi      0x001068 6295656  rdi      0x7fffffffddc30 140737488346160  rcx      0xa616c6f 174156011  rdx      0x0 8  0x7fffffffddc00 0x7fffffffddc00
r8        0x002675 6301301  r9        0x7fffffffdd500 140737354003712  rbp      0x400890 0x400890 <__libc_csu_init>  rsp      0x240 582
r12       0x400640 4195904  r10       0x7fffffffdd500 140737354003712  r10      0x602010 6299664  r11      0x0 0
rip       0x4007ce 0x4007ce <main+115>  r13       0x7fffffffdd080 140737488346496  r14      0x0 0  r15      0x0 0
ds        0x0 0  eflags    0x200 [ PF IF ]  cs        0x33 51  ss        0x2b 43  gs        0x0 0
es        0x0 0

0x4007a7 <main+76> mov $0x64,%esi
0x4007ac <main+81> call 0x400600 <fgets@plt>
0x4007b1 <main+86> test %rax,%rax
0x4007b4 <main+89> je 0x400785 <main+42>
0x4007b6 <main+91> movb $0x52,0x2008ab(%rip) # 0x601068 <password>
0x4007bd <main+98> lea 0x30(%rsp),%rdi
0x4007c2 <main+103> mov $0x3,%edx
0x4007c7 <main+108> lea 0x20089a(%rip),%rsi # 0x601068 <password>
> 0x4007ce <main+115> call 0x4005d0 <strncmp@plt>
0x4007d3 <main+120> test %eax,%eax
0x4007d5 <main+122> je 0x4007dc <main+129>
0x4007d7 <main+124> call 0x400727 <boom>
0x4007dc <main+129> lea 0x20(%rsp),%rdi
0x4007e1 <main+134> mov $0x0,%esi
0x4007e6 <main+139> call 0x4005f0 <gettimeofday@plt>
0x4007eb <main+144> mov 0x20(%rsp),%rax

native process 6980 In: main
0x0000000000400796 in main ()
0x000000000040079b in main ()
(gdb) nl
0x00000000004007a8 in main ()
0x00000000004007a7 in main ()
0x00000000004007ac in main ()
0x00000000004007b1 in main ()
(gdb) nl
0x00000000004007b4 in main ()
0x00000000004007b6 in main ()
(gdb) nl
0x00000000004007bd in main ()
0x00000000004007c2 in main ()
0x00000000004007c7 in main ()
0x00000000004007ce in main ()
(gdb) p (char*) 0x601068
$10 = 0x601068 <password> "Rorrecta"
(gdb)
```

Ejecutamos un run con un br *main y tras pedirnos la contraseña justo antes de la comparación de cadenas por strncmp se hace un mov y un lea, usamos p(char*) 0x601068 y observamos que la contraseña es Rorrecta.

```
Actividades - Terminal - Vie 21:41
juse@juse-OMEN-by-HP-Laptop: ~/Escritorio/Universidad_ubuntu/EC/Practica4/Bombas_resueltas/Maria_Alcazar_Marcos

--Register group: general
rax      0x1 1  rbx      0x1 1  rcx      0x10 16  rdx      0x7fffffffdd160 140737351850192
rsi      0x1 1  rdi      0x0 0  rbp      0x400890 0x400890 <__libc_csu_init>  rsp      0x7fffffffddc00 0x7fffffffddc00
r8        0x0 0  r9        0x0 0  r10      0x7fffffffdd2cc0 140737349430464  r11      0x400800a 4196874
r12       0x400640 4195904  r13      0x7fffffffdd080 140737488346496  r14      0x0 0  r15      0x0 0
rip       0x40084a 0x40084a <main+239>  eflags    0x240 [ PF ZF IF ]  cs        0x33 51  ss        0x2b 43  gs        0x0 0
ds        0x0 0  es        0x0 0  fs        0x0 0

0x40084a <main+239> imul $0x3,0xc(%rip),%eax
0x40084f <main+244> cmp 0x20080b(%rip),%eax # 0x601060 <passcode>
0x400855 <main+250> je 0x40085c <main+257>
0x400857 <main+252> call 0x400727 <boom>
0x40085c <main+257> lea 0x10(%rsp),%rdi
0x400861 <main+262> mov $0x0,%esi
0x400866 <main+267> call 0x4005f0 <gettimeofday@plt>
0x40086b <main+272> mov 0x10(%rsp),%rax
0x400870 <main+277> sub 0x20(%rsp),%rax
0x400875 <main+282> cmp $0x5,%rax
0x400879 <main+286> jle 0x400880 <main+293>
0x40087b <main+288> call 0x400727 <boom>
0x400880 <main+293> call 0x400741 <defused>
0x400885 nopw %cs:0x0(%rax,%rax,1)
0x40088f nop
0x400890 <__libc_csu_init> push %r15

native process 12559 In: main
(gdb) layout regs
(gdb) p (int) 0x601060
$1 = 6295640
(gdb) p (int) 0x601060
$2 = 23331
(gdb)
```

Vamos a `br *main+239` y se ve que multiplica por 3 el valor, si hacemos `p {int} 0x601060` nos da 23331 que pone como etiqueta passcode, sin embargo sabemos que ha sido multiplicado por 3, por lo tanto el verdadero pincode es `p {int} 0x601060 = 23331` dividido entre 3 que sale 7777.