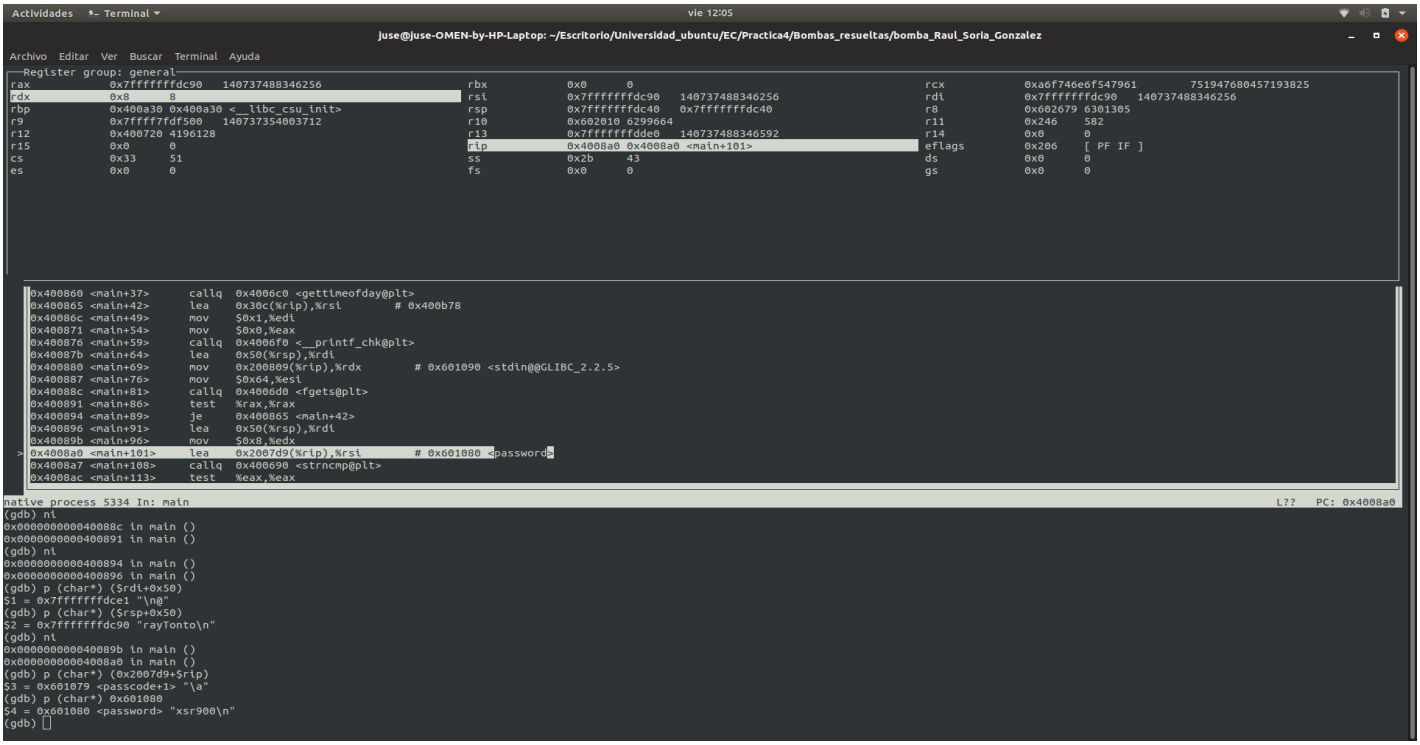
Pratica 4: Bombas resueltas

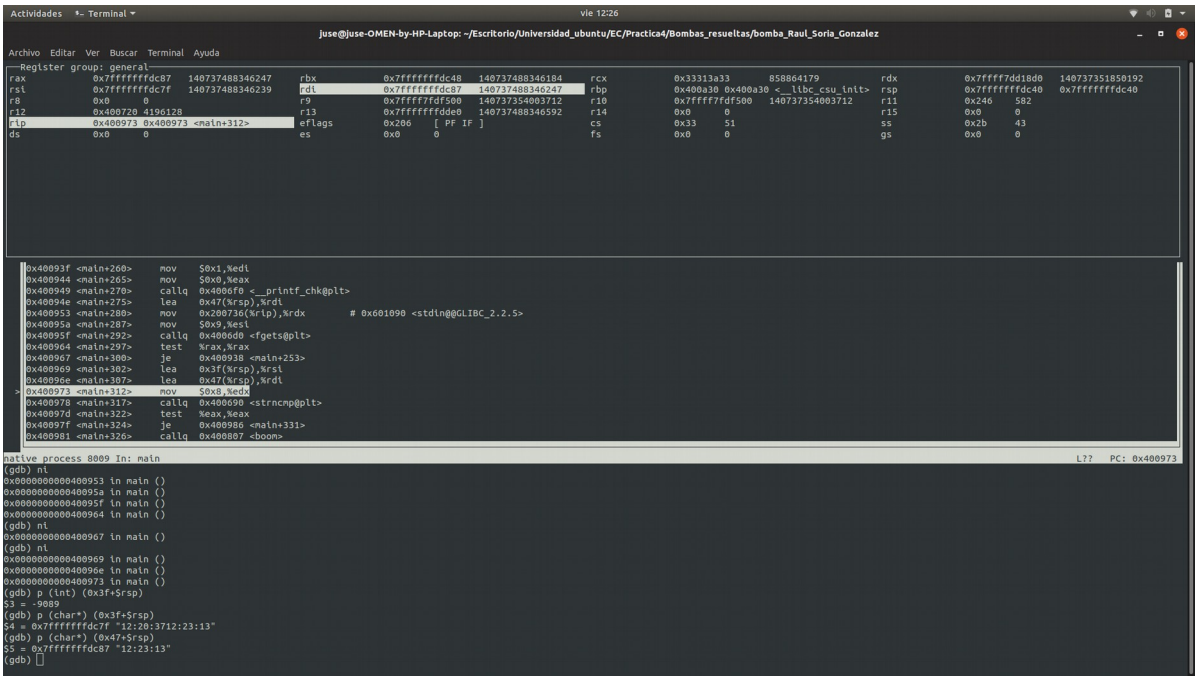
- **Bomba Raúl Soria González**

  Contraseña:xsr900 Pincode:1998

  En primer lugar hice un br *main y run hasta llegar a la llamada de strcmp, llamé a p (char*) 0x601080 que tiene la etiqute de password y me mostró la conraseña que es: xsr900.



  Tras probar la contraseña te pide que le des la hora, el minuto y segundo en que la introdujiste, usando gdb y con el br *main+300 ves que
  p (char*) (0x47+$rsp) y te devuelve 12:23:13 que es lo que he puesto yo
  p (char*) (0x3f+$rsp) te devuelve 12:20:37 12:23:13 y entonces vemos cual es el que hay que poner, que es 12:20:37 el momento exacto.



Saltado ya el pasado de la hora, vemos como compara el pin introducido con p*(int*)(0xc+$rsp) y vemos que es 1998.

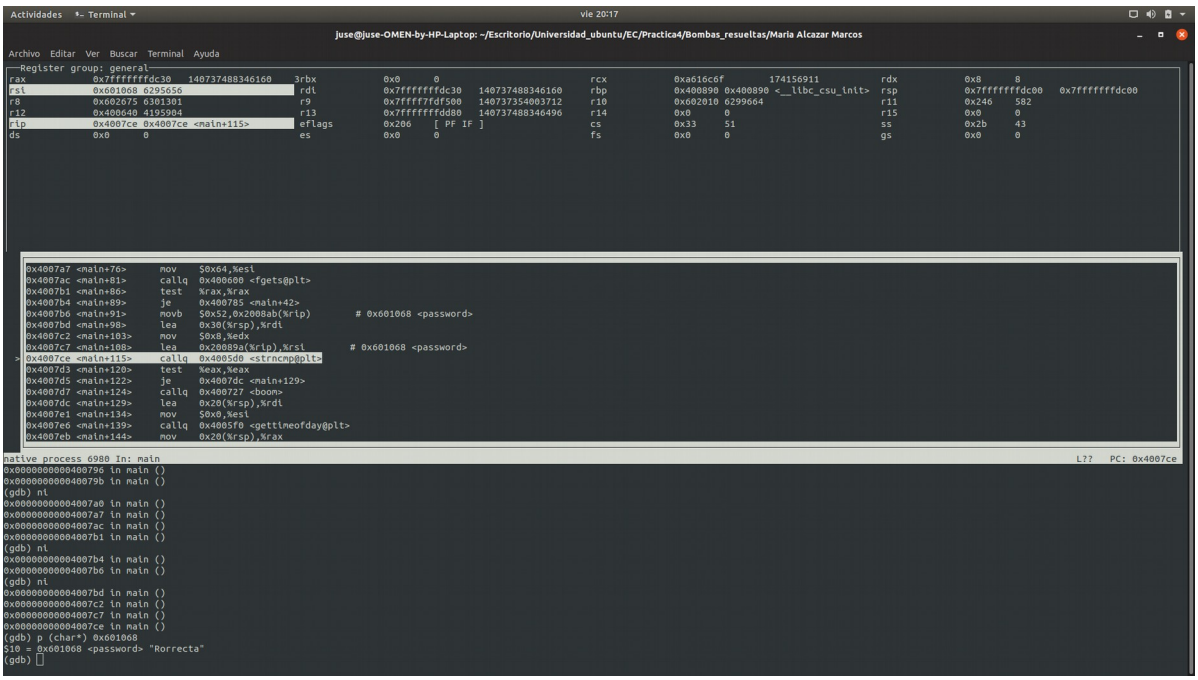
- **Bomba Alberto Villanueva Copado**

  Contraseña:contrasenia Pincode:1221

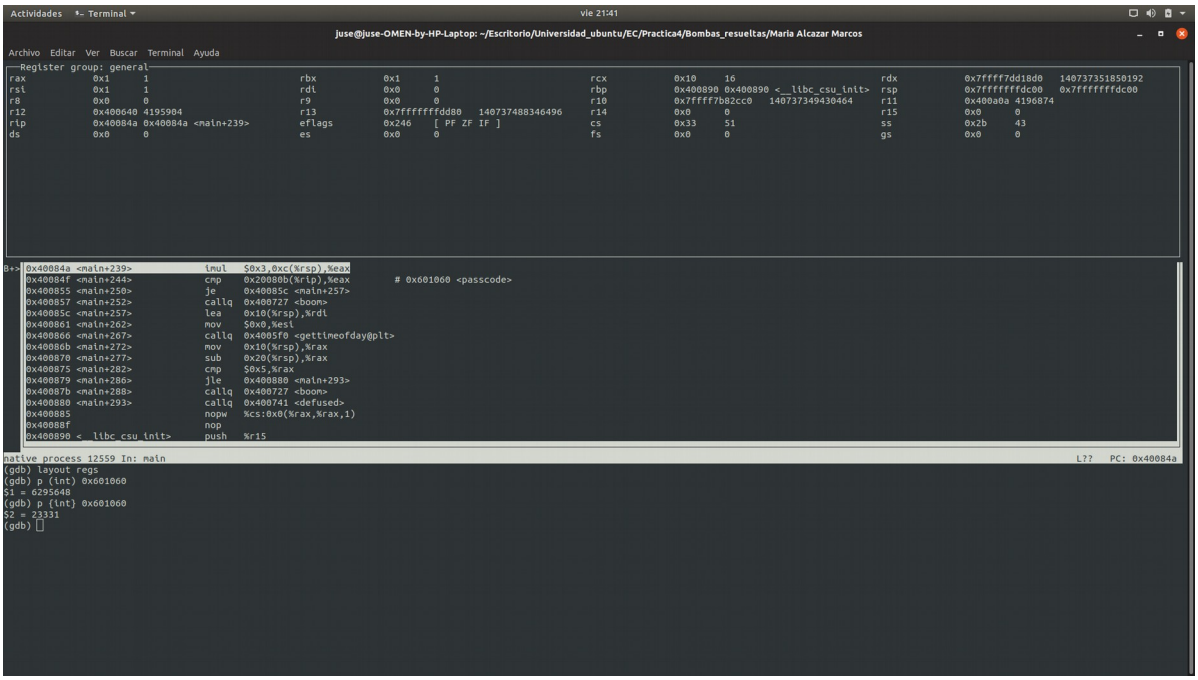
  Seguimos el mismo procedimiento de la anterior bomba, ponemos un br *main y run. Con ni llegamos hasta la dirección 0x400962 y observamos que el valor del registro %rsi es contrasenia.
  Tras obtener la cotraseña seguimos hasta la dirección 0x400a5e y ahí se compara el pin, hacemos p (int) $eax y obtenemos 1221 que es el pincode

- **Bomba María Alcázar Marcos**

  Contraseña:Rorrecta Pincode:



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.



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 dividio entre 3 que sale 7777.