David Criado Ramón

Las claves son: dontbPlz y 2016.

Para resolverlo:
1) Buscamos el punto de entrada de datos para la cadena inicial. (main <+79>)

2) Comprobamos que ocurre con los argumentos hasta que llegamos a strncmp (main <+136>).

Podemos comprobar a 0x70 por debajo de %ebp (lugar en el que podemos comprobar que empieza la cadena) se le resta un carácter. Análogamente ocurre con 0x6c por debajo de %ebp que se corresponde con el cáracter que ocupa la posición 4 (Si consideramos la posición cuatro primero). Por tanto nos quedaría que a la cadena que hemos introducido se le disminuyen en uno el carácter 0 y el carácter 4.

3) Justo después de ver los dos decrementos se realiza un strncomp, miramos las direcciones en las que estás las cadenas y vemos que que se hace un push de una dirección de memoria (0x804a040).

4) Como esa dirección contenía “contaPlz”, para contrarrestar la resta sumamos en nuestra entrada y nos quedaría “dontbPlz”.

5) Buscamos el punto de entrada del código numérico. (main <+221>)

6) Vemos que desplaza aritméticamente a la derecha una vez (divide por 2) el número introducido y luego resta 8.

7) Justo antes de la explosión compara %eax con %edx (lugar donde esta nuestro número). Como en %eax carga una posición de memoria poco antes de la comparación analizamos dicha posición de memoria y vemos que el número que hay en ella es 1000.

8) Por tanto si realizamos el camino hacia atrás sustituyendo la resta por suma y la división por la multiplicación (o desplazamiento arimético a derecha con izquierda, como prefiera verlo). Nos quedaría que el dígito a encontrar era (1000+8) * 2 = 2016