Laboratorio #1

José Arturo García Rodríguez

Rebeca Servellón Orellana

Diego Jiménez Chamorro

Preguntas

1. ¿Se visualiza en pantalla el resultado que esperaban?
    a. Sí.
2. ¿Pueden explicar cómo funciona el '|' en la instrucción anterior? ¿Pueden describir qué hace grep? ¿Qué ocurre si se elimina '| grep A-20 main.:' de la instrucción? Finalmente, ¿pueden describir la salida de la instrucción?
    a. Un "O" lógico
    b. Decompila el código
    c. Decompila el programa
    d. La salida se puede tomar como el código Assembly que se convierte del código C
3. ¿Pueden explicar cómo funciona el '|' en la instrucción anterior? ¿Pueden describir qué hace grep? ¿Qué ocurre si eliminan '| grep A-20 main.:' de

la instrucción? Finalmente, ¿pueden describir la salida al ejecutar esa instrucción y determinar si el código está 32-bit o 64-bit?

   a. Un “O” lógico
   b. Decompila el programa
   c. La primera línea del comando con el grep dice “64”, pero el profesor explicó que se podía determinar por un “r” al inicio de las instrucciones Assembly

4. ¿Qué es gdb? De la información desplegada después de ejecutar esas instrucciones, ¿pueden encontrar cuáles son los registros de propósito general del CPU? ¿Pueden identificar los registros stack pointer, base pointer, source index y destination index? ¿De qué tamaño son los registros que se observan en la salida? ¿Cuál de esos apuntadores es el que lleva en el CPU la instrucción que se está leyendo en ese momento?

   a. El debugueador
   b. Sí
   c. En la salida aparece “rsp”, “rbp”, “rsi” y “rdi”
   d. Son 4 bytes en el primer segmento y 4 bytes en el segundo segmento; por lo tanto, corresponden a 8 bytes en total
   e. Se conjetura que es base pointer

5. ¿Pueden interpretar el código en ensamblador y entender el flujo con respecto al programa codificado en C? ¿Qué información contiene el registro rip?
    a. Se puede observar cierta similitud con algunas líneas de código, como en la parte que dice “puts”. Además, se puede observar que hay un ciclo, porque el código se devuelve a cierto punto si el jle no cumple la condición.
    b. El valor de la siguiente instrucción, como todo se va metiendo al stack, entonces cuando termina de ejecutar todos los bloques apilados y vuelve al primer bloque que se ingresó, se tendría el retorno.
6. ¿Cómo almacena el procesador las variables: little-endian o big endian? ¿Qué tipo de información permiten visualizar los comandos anteriores?
    a. En distintos formatos según se requiera, en los comandos se visualizan los formatos hexadecimales y decimales (positivos).
    b. El ‘4’ de los comandos especifica el número de elementos que se visualizarán. Por otra parte, “xb” está compuesto por x (hexadecimal) y “b” de byte. En adición, “ub” está compuesto por u (unsigned decimal) y “b” de byte. Finalmente, “xw” está compuesto por w (hexadecimal) y w (Word-32bits). Por lo tanto,

se concluye que se está visualizando la dirección de memoria a la que apunta el registro “rip” en distintos formatos

7. ¿Qué información les proporciona la salida de estas instrucciones?

a. El instruction pointer va indicando la siguiente instrucción a ejecutar según avanza en el programa, al empezar el programa empieza desde la dirección de memoria de main

b. La dirección del instruction pointer cuando está en la primera instrucción dentro del main, que sería la de comparar el valor del iterador con el límite del ciclo for

c. Las direcciones que comprende el instruction pointer cuando el iterador es igual a 3

8. ¿Qué información les proporciona la salida de las instrucciones? ¿Podrían completar la ejecución del programa paso a paso? ¿Podrían determinar en cuál segmento de memoria del programa se almacena el código de la función puts, y en cuál dirección? ¿En cuál dirección de memoria está almacenada la variable i, y en cuál segmento de memoria?

a.

b. Sí

c. puts se ubica en el segmento de código/texto en la dirección

   0x555555555165

d. La variable i se encuentra almacenada en el stack en la dirección de memoria 0x7fffffffdf88. El next i funciona para mostrar la siguiente instruccion