PES UNIVERSITY

(Established under Karnataka Act No.16 of 2013)

100-ft Ring Road, BSK III Stage, Bangalore 560 085

Department of Computer Science

Session: Jan-May 2021

UE19CS254: Operating Systems

Assignment 3

1. Use Program 1 of Assignment 1 to do the following:

   a) Note the size of the text, bss, and data segments in the corresponding object file. Add necessary types of variables to the program and showcase the growth of the each segment.

   b) Generate the corresponding map file. Interpret the map file to analyse the memory map of the text section, bss section, and user defined variables.

2. Use Program 1 of Assignment 1 to do the following:

   a) Examine the memory using gdb to obtain the address where the variables are stored. What is stored in each byte of the address? Identify the endianess of the data stored.

   b) Make use of 'x/30i main' and 'x/30x main' gdb instructions. Examine all the memory addresses listed and their content.

3. For Program 1 of Assignment 2, use objdump to analyse the program binary. Identify the memory addresses in use, machine language instructions, and assembly instructions. Analyse the register contents by stepping through the program exactly as it is run on the machine. Explore the various threads and their associated data as well. (Employ suitable break points and 'nexti', 'x/i $rip' instructions may be used.)

Questions

1. Uninitialized and initialized variables are stored in the … and … segment and of a C program respectively.
   a. Text, Data
   b. Data, BSS
   c. BSS, Data
   d. BSS, Text

2. Function call return addresses are stored in the …. segment and shared libraries are stored in the …. segment respectively.
   a. **Stack, Heap**
   b. Stack, BSS
   c. Heap, BSS

d. Heap, Stack

3. For debugging with GDB, the compiled program can be run by the command
   a. execute
   b. **run**
   c. ./<filename>
   d. None of the above

4. For debugging with GDB, the value of a local variable can be assigned using
   a. **set**
   b. assign
   c. init
   d. None of the above

5. To display the contents of the symbol table, the following command can be used
   a. objdump -f objfile
   b. objdump -h objfile
   c. **objdump -t objfile**
   d. objdump -p objfile

Additional Material

1. https://www.embeddedrelated.com/showarticle/900.php
2. https://www.geeksforgeeks.org/memory-layout-of-c-program/
3. http://www.unknownroad.com/rtfm/gdbtut/gdbtoc.html
4. https://bob.cs.sonoma.edu/IntroCompOrg-RPi/sec-gdb1.html
5. https://perspectiverisk.com/intro-to-basic-disassembly-reverse-engineering/