CentOS Virtual Machine

4 (a). Objdump used to list shared object libraries.



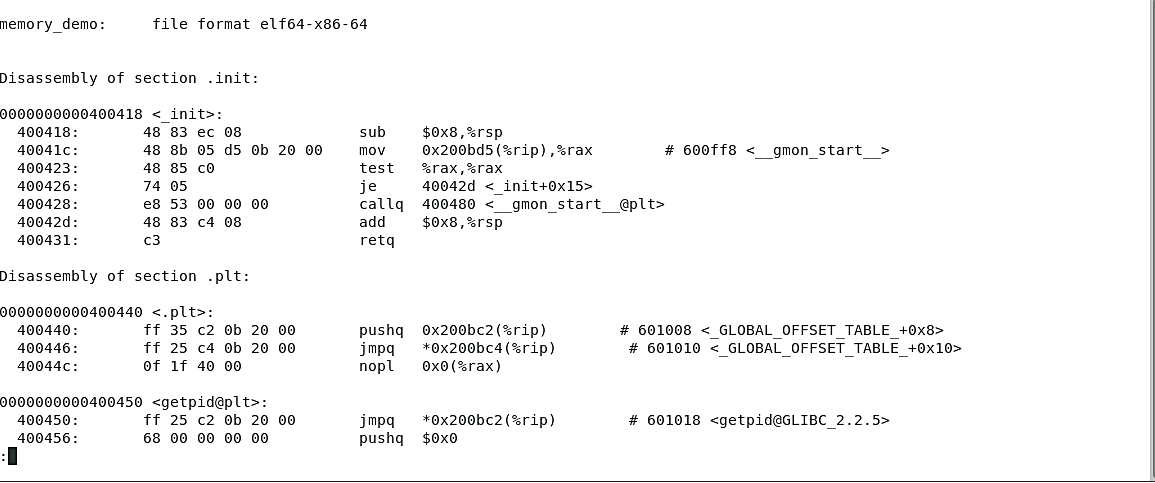
Graphical user interface

Description automatically generated with low confidence4 (b). ldd to see a list of shared object libraries before executing compiled program.

Text

Description automatically generated4 (c). Inspect all memory section header.

4 (d). Disassembling compiled machine code to make it more readable. Using objdump -d.



4 e. ‘hexdump -C memory\_demo | less’ command to display hexadecimal contents of the file



Table

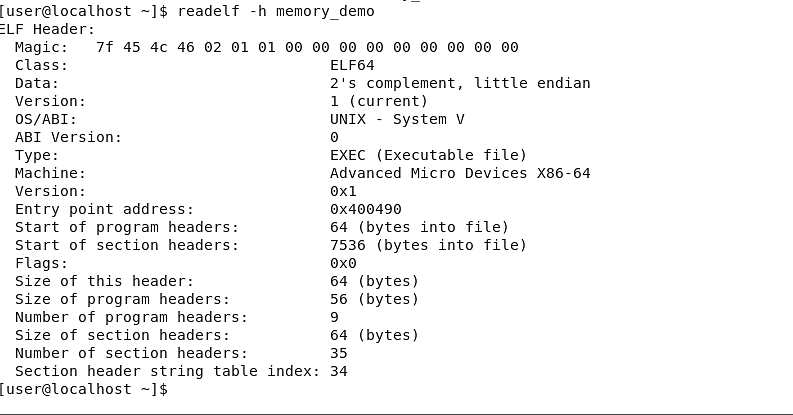
Description automatically generated

5. Results of ‘size’ command

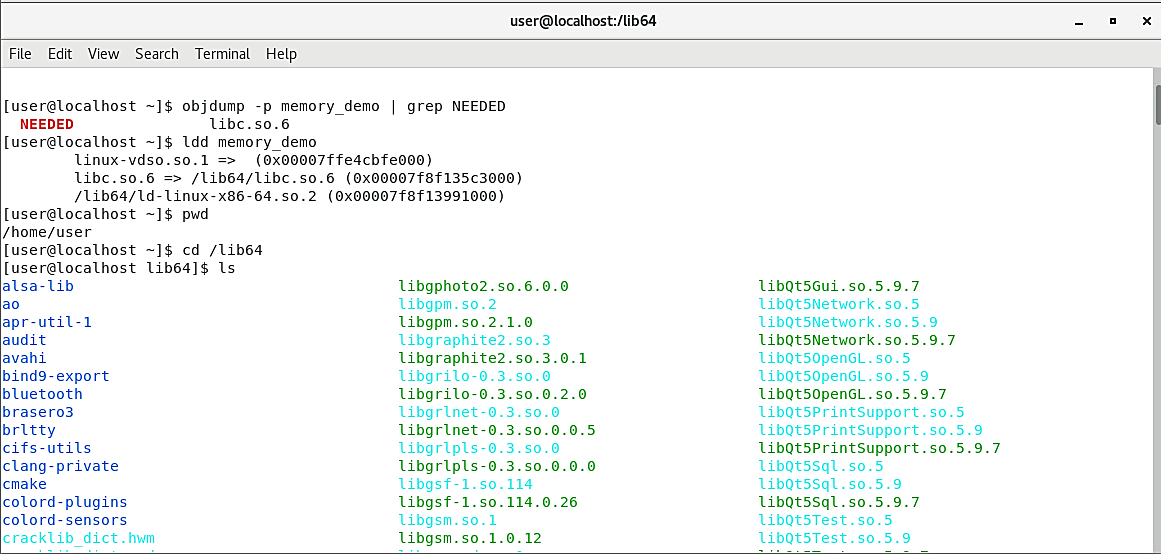
Graphical user interface, application

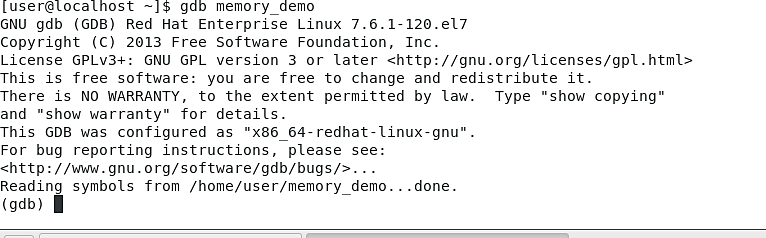
Description automatically generated

6. Results of ‘readelf -h memory\_demo’.

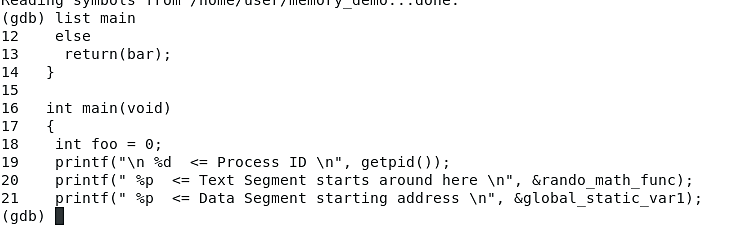


7. I located the actual shared object files by running the ldd memory\_demo and objdump -p commands. Then, I determined that /lib64/ had the files. I used cd command to change directory to the desired one (cd /lib64). Then I used the ls command to list the shared files in the directory lib64.



8. Using ‘gdb’ to debug the program.

9. Listing the main function.



10. Disassemble rando\_math\_func.

Text

Description automatically generated with medium confidence

11. Setting a breakpoint then running/executing the program inside the debugger until it hits the breakpoint (using r command).

Text

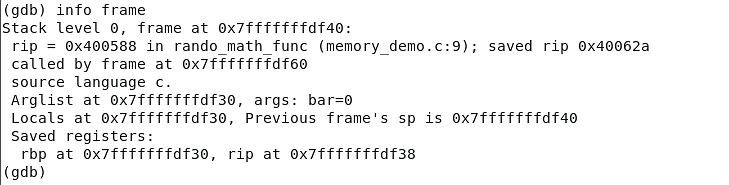
Description automatically generated

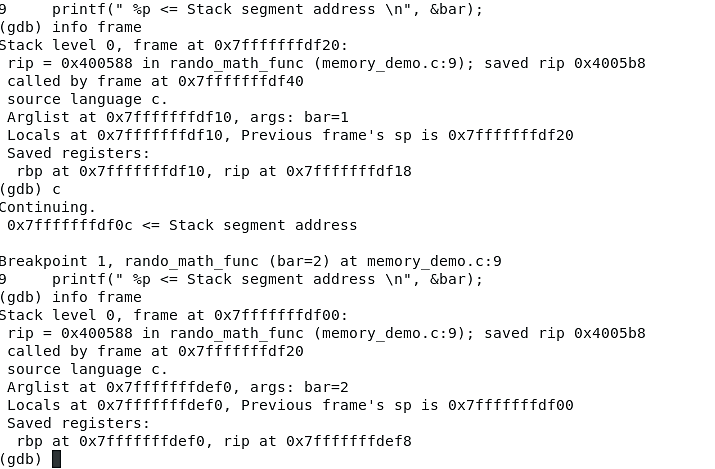
12. Inspecting the registers. The rsp (highlighted) refers to the Stack Pointer value and the rbp (circled) refers to the Base Pointer value. The stack pointer value points to the top of the current stack frame while the base pointer refers to the base of the current stack frame.

Table

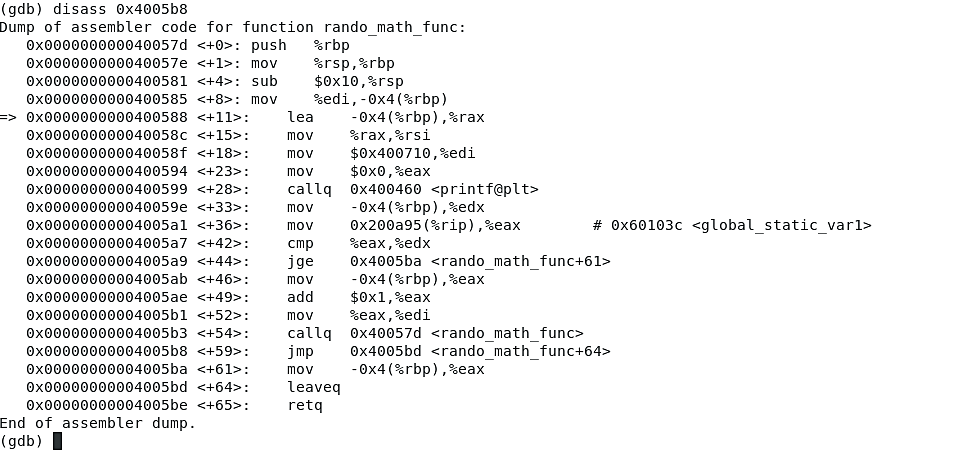
Description automatically generated

13. Inspecting the context of the current frame.

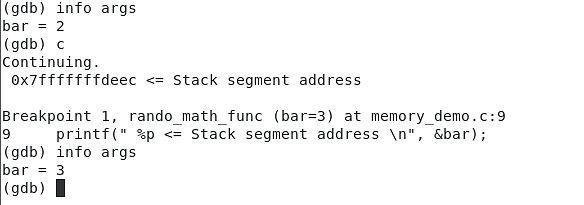
13 (b). Continuing execution then hitting the same breakpoint again. Doing a second info frame.



14. Disassembling code near ‘saved rip’ address.

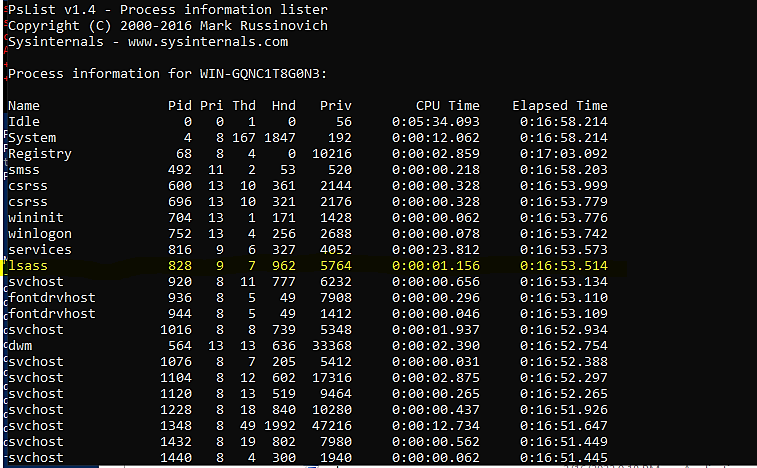


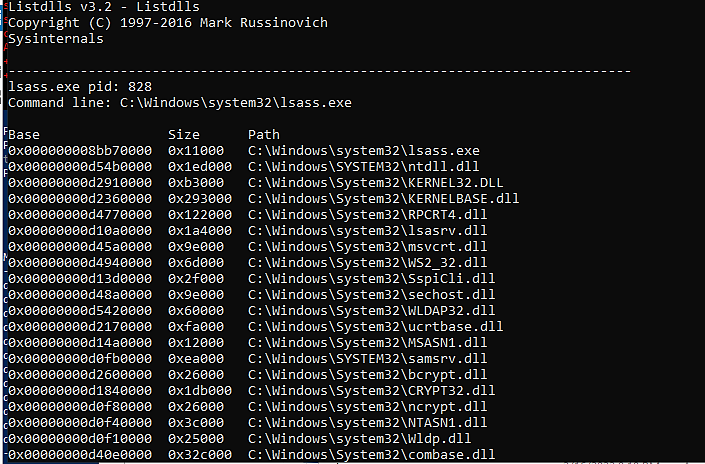
15. Exploring ‘info args’ through two iterations.



Windows Server 2019

4. Obtaining a process list in the SysInternalsSuite directory. The process ID of the Isass process is 828 (highlighted).



5. Isass.exe mapped DLLs.

7. Screenshot of VMMap. The memory marked for “Execute/Read” permissions is found under the Protection column in the bottom window and is under Type “Image”.

