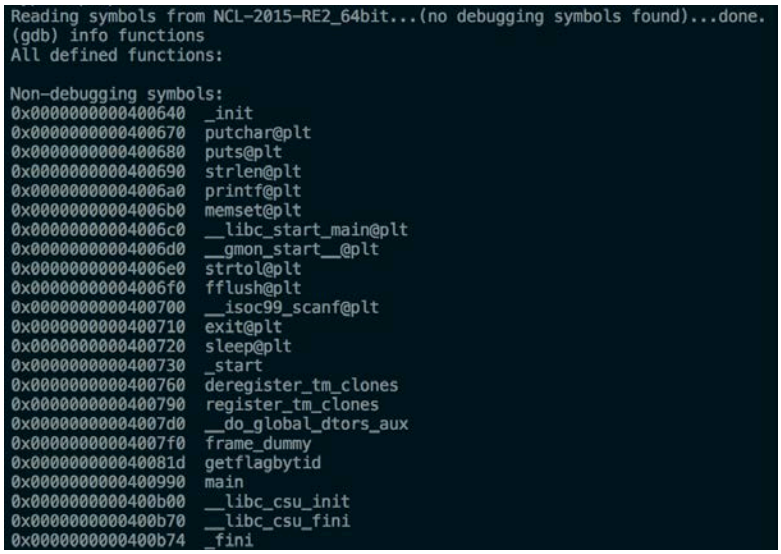
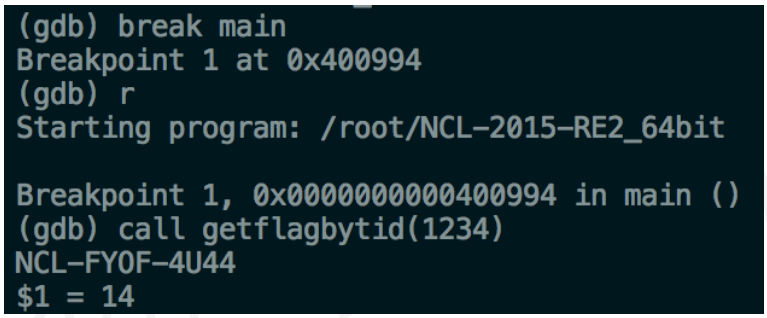
Enumeration and Exploitation

Binary 2 (Hard)

This challenge evaluates the contestant's ability to use a debugger to exploit a compiled binary. One possible tool to use is the "GDB" Linux program. A Linux binary is provided and the contestant is tasked with extracting the secret flag. This can be solved by attaching GDB to the provided binary to help search for any clues in the program. The GDB command, "info functions" will return a list of all the functions that are in scope. This list contains an interesting function called "getflagbytid" and can be called by breaking on line 1 of the main function and using the "call" command in GDB.





Question	Answer
What is the flag hidden in the program?	NCL-FYOF-4U44

© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.