Bomb Lab Recitation

Fall 2023

Outline

- Introduction
- Getting Started
- Running the Bomb
- Useful Commands
- Tracing Assembly with gdb
- Resources, Tips

Introduction

- Goal: Deactivating “bombs”, compiled binaries that you need to enter specific strings to “defuse” phases.
- 6 phases in each bomb, each bomb has different set of phases and solution strings.
- Practice your assembly reading skills and understand the way compiler converts C to x86.

Getting Started

- Get the bomb from: http://cakpak2.ceng.metu.edu.tr:15213
- You have to be on the campus network or use METU VPN for your connection.
- To get the bomb you need:
- Username: 6 digit username: eXXXXXX
  - No other username will be accepted.
- Email: Any proper email that is reachable

Rules

- You are NOT allowed to get multiple bombs.
- If you do so, your lowest grade bomb will be considered while grading.
- Moreover, we will count the total number of explosions of your bombs.
- Grade = MIN(bombgrades) - SUM(explosions) * 0.5

Running the Bomb

- You can run the bomb on inek machines from [1,100]. You are not allowed to use your personal computers for this homework.
- You can put your bombs to inek machines using sftp or scp.
- And work on the inek machines from home using ssh.
- Your important actions (bomb defusals, explosions) will be notified to the bomb server. You can follow them from: http://cakpak2.ceng.metu.edu.tr:15213/scoreboard

Useful Commands

- objdump -d Disassembles instruction related parts of the object file.
- strings prints printable strings of length >= 4 found in the file.
- objdump -t prints the symbol table of the object file.
- Various gdb commands for debugging and assembly inspection.
- gdb bomb := start gdb with bomb
- gdb> run := run program with cmd_args
- gdb> break := put a break point to the specified label or addr
- gdb> info break := list active breakpoints
- gdb> delete <#> := delete breakpoint with number “#”
- gdb> continue := run program until a breakpoint is hit
- gdb> stepi := run a single instruction
- gdb> nexti := run a single instruction, if it is a function call, run program until function returns
- gdb> kill := terminate the program
- gdb> disas := lists assembly code of the current function
- gdb> disas := lists assembly around instruction addr, label or for the whole function.
- gdb> print ($rsp) := print contents of %rsp as decimal signed number
- gdb> tui <enable/disable> := enables/disables a more gui like view
- gdb> layout <asm/regs/source> := changes tui view to your liking
- gdb> focus <asm/regs/cmd> focuses cursor for the specified window in tui mode.

Resources and Tips

- A cheat sheet about GDB: gdbnotes-x86-64.pdf
- Chapter 3 of the textbook
- Read homework instructions carefully, there are some tips and important details there.