

Ghidra SRE Challenge with NSA

Clayton B. Hodges

Colorado Mesa University

CSCI 420: Software Security

Contents

1. Task Completion..... 2

1.1 Instructions..... 2

1.2 Puzzle..... 2

1.3 Black Box..... 6

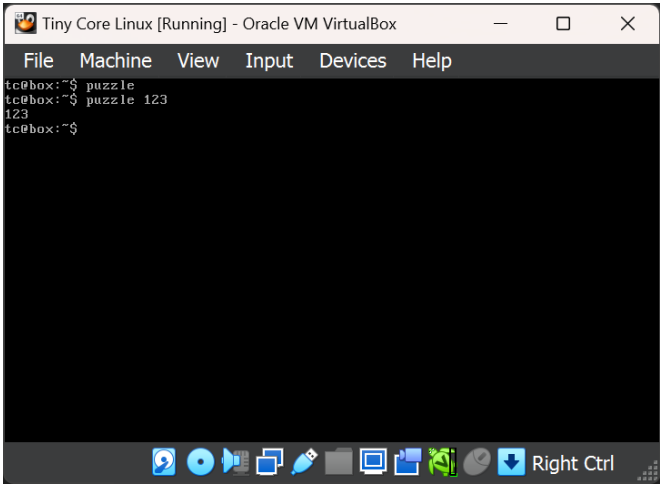
1. Task Completion

1.1 Instructions

- I. Install Ghidra, VirtualBox, and materials.
- II. Launch Tiny Core Linux and test executable(s) inside.
- III. Launch Ghidra, create a project, and upload executable(s).
- IV. Use Ghidra to deconstruct the executable(s), break down binary functions, and discover secrets.

1.2 Puzzle

- I. Entering 'puzzle' and 'puzzle 123' in Tiny Core Linux.

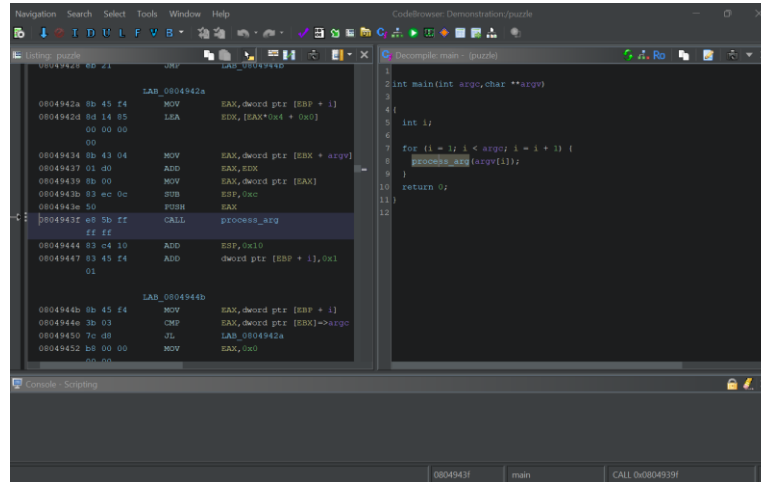


```
Tiny Core Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
tc@box:~$ puzzle
tc@box:~$ puzzle 123
123
tc@box:~$
```

(Puzzle's expected output when run directly is nothing, but it prints any args it's passed.)

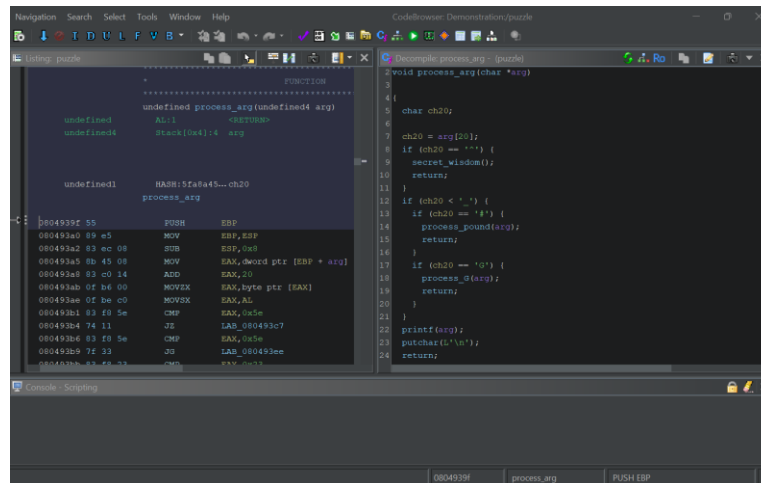
GHIDRA SRE CHALLENGE

II. Investigating Puzzle's deconstructed contents and relabeling content in Ghidra.



(The main entry point of the program calls a function we labeled process_arg.)

III. Further investigating Puzzle functions.

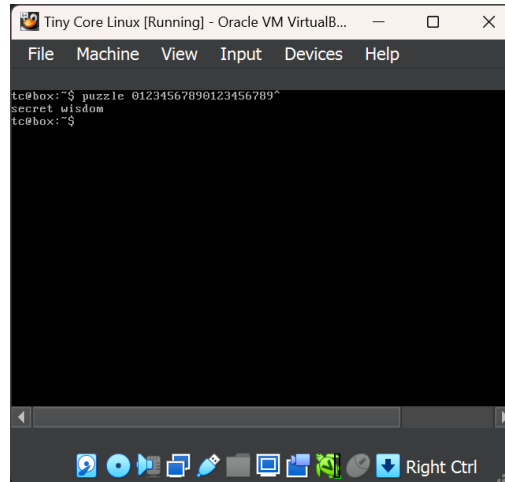


(The function(s) called by main are further examined, revealing that passing a string with '^' at

arg[20] to Puzzle will result in secret message output.)

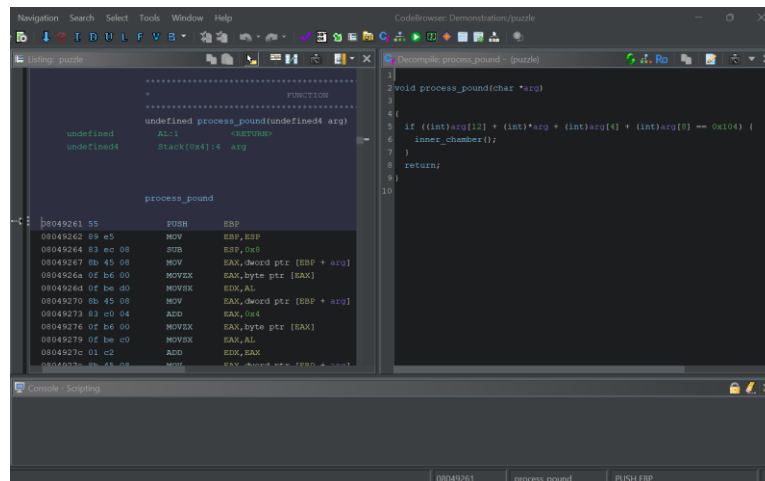
GHIDRA SRE CHALLENGE

IV. Entering 'puzzle 01234567890123456789^' in Tiny Core Linux.



(Puzzle prints 'secret wisdom' instead of the expected output.)

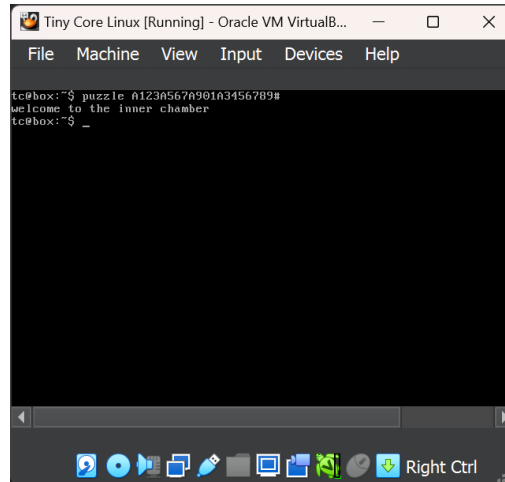
V. Further investigating Puzzle functions.



(Upon further investigation, a function reveals that passing '#' at arg[20] and ASCII values that add up to 260 at arg[0], arg[4], arg[8], and arg[12] to Puzzle will result in the output of a secret message.)

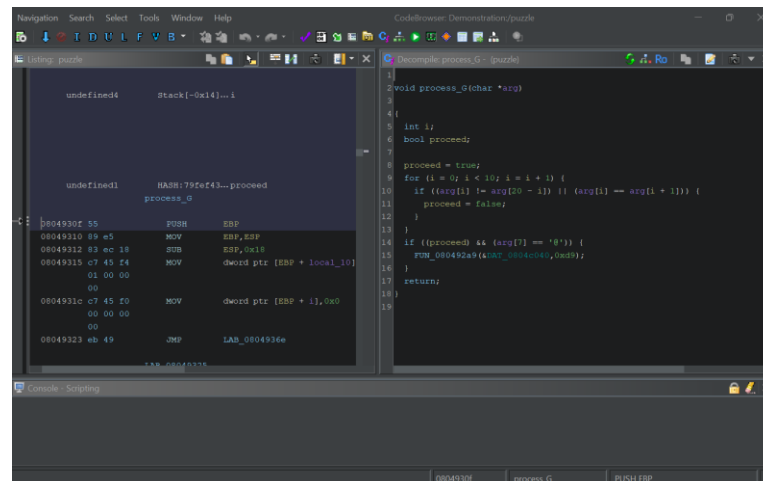
GHIDRA SRE CHALLENGE

VI. Entering 'puzzle A123A567A901A3456789#' in Tiny Core Linux.



(Puzzle prints 'welcome to the inner chamber' instead of the expected output.)

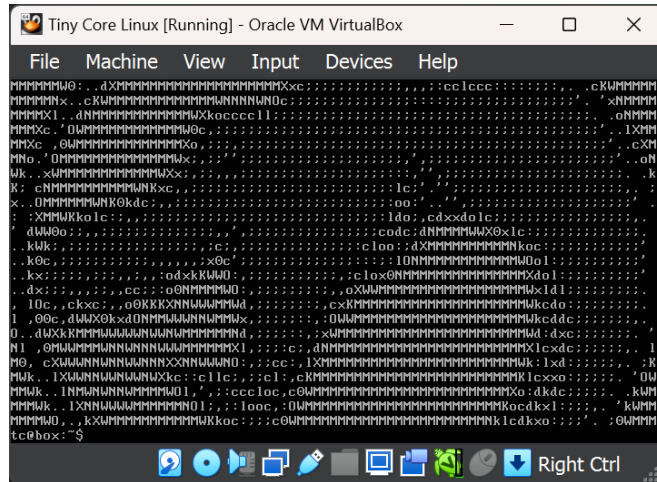
VII. Further investigating Puzzle functions.



(Upon further investigation, a function reveals that passing 'G' at arg[20] and '@' at arg[7] to Puzzle and ensuring the rest of the argument is a palindrome without repeating characters will result in the output of a secret message.)

GHIDRA SRE CHALLENGE

VIII. Entering 'puzzle GBABABA@ABABA@ABABABG' in Tiny Core Linux.



(Puzzle prints ASCII art of the Ghidra logo instead of the expected output.)

1.3 Black Box

I. ...