Secure and Dependable Systems

Assignment 2

Spring 2020

Raja Rafey and Huzaifa Hashim

Problem 1: Program to calculate basic statistics

The code in main.c takes in an arbitrary set of values from the terminal and computes the statistics. The executable is located under:/build/ds.

In order to test the executable, pass a string via a pipe to the executable. /ds with the corresponding command line arguments:

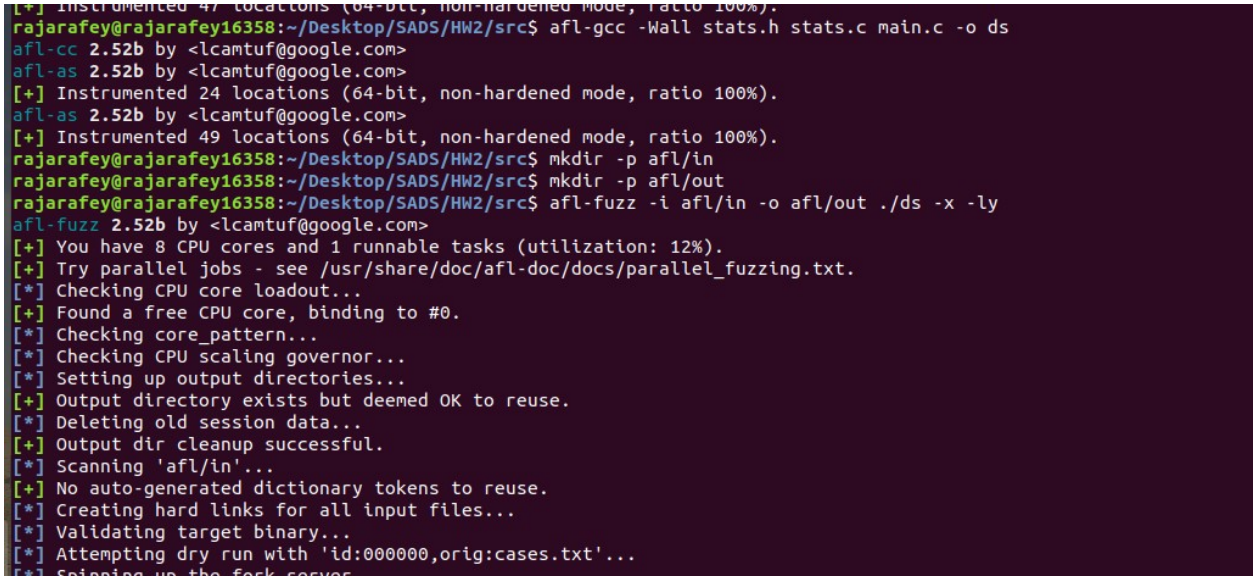
printf"1 2 3 12\n4 5 6\n7 8 9\n" | ./ds min 0 max 0 min 1 max 1...

Problem 2: Fuzzing using American Fuzzy Lop

a) The instrumentation of this code is done by compiling using the following command in the directory where the source code for main.c resides:

afl-gcc –Wall stat.h stat.c main.c –o ds

This instruments the code and gives out the following result before we run the fuzzer:



b) Seed Cases are piped into the fuzzer program as inputs in the form of matrices in different files. The first input is the best case scenario where the program is given an n*n matrix, which our front-end converts to column vectors, and computes the statistics of using the functions already written in class. The following inputs then provides incomplete matrices, which are bound to fail, because the traversals of such matrices result in column vectors which are unevenly distributed as a result of transposing said matrix.

To run the fuzzer, we create a directory for afl/out and afl/in after which we can execute the command to run the fuzzer, assuming that our executable resides in /src/ds:

```
afl-fuzz –i afl/in –o afl/out ds –x -ly
```

c) After running the fuzzer for a brief 17 minutes, we noticed that the fuzzer could not find a unique path for a crash for a considerably long time at the latter half of the 17 minute. The stability of the program after running falls to 58.73%, however, the documentation for the Fuzzer says the following about stability:

```
When the value is lower but still shown in purple, the fuzzing process is
unlikely to be negatively affected. If it goes into red, you may be in
trouble, since AFL will have difficulty discerning between meaningful and
"phantom" effects of tweaking the input file.
```

Thus, since the number is still purple, it means the fuzzing is not negatively effected in the first 17 minutes of its running.