COMSM0049 Lab 6

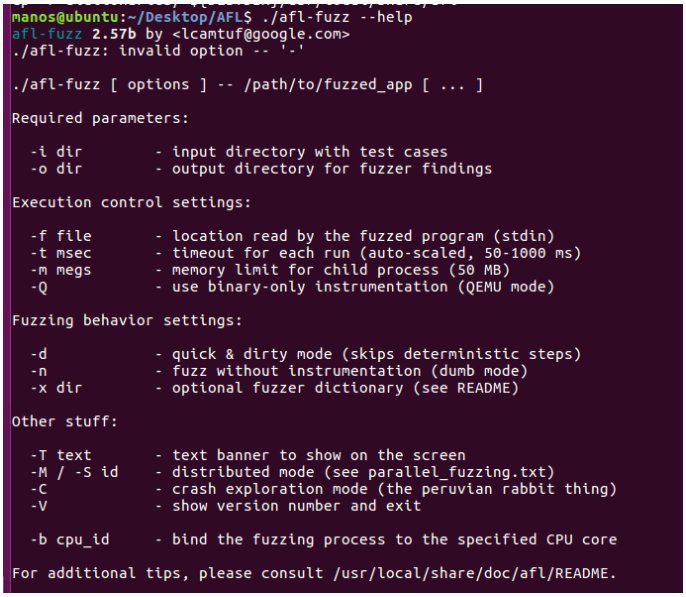
1. Download and compile AFL:

git clone https://github.com/google/AFL

cd afl

make && sudo make install

2. check if afl-fuzz and afl-gcc are working:



3. create these subdirectories in the root directory:

$ mkdir temp-in

$ mkdir temp-out

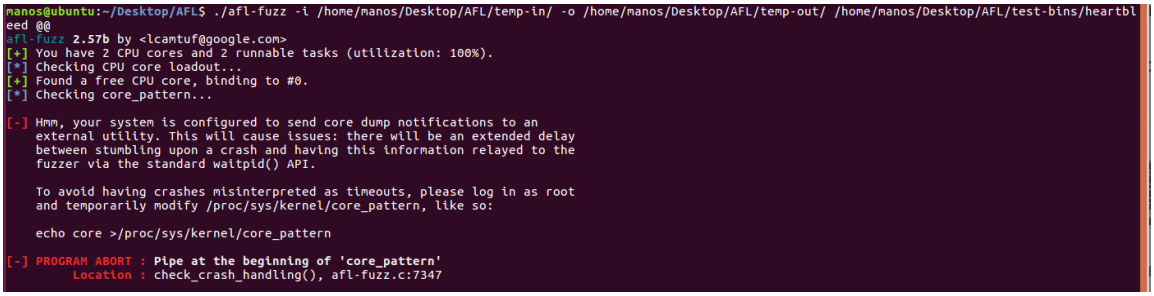
$ mkdir test-bins

3. Move heartbeat_normal.bin into temp-in:

4. Compile heartbleed.c

5. Run AFl fuzzer: ./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o

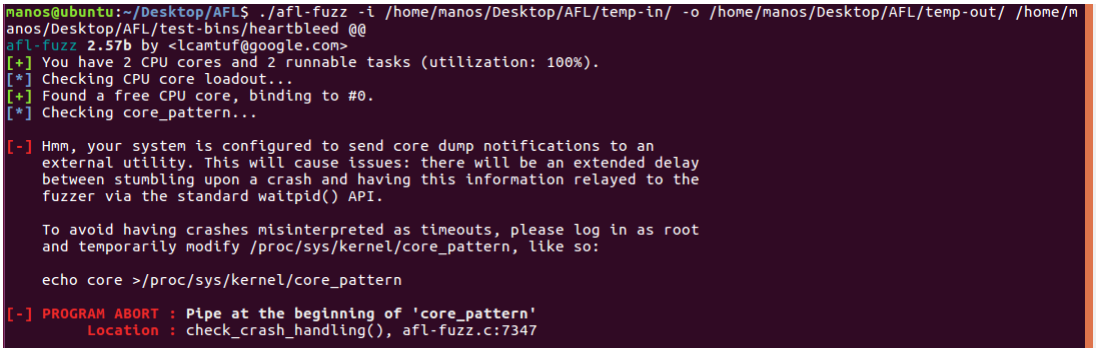
/home/manos/Desktop/AFL/temp-out/ /home/manos/Desktop/AFL/test-bins/heartbleed @@



Fix:

echo core | sudo tee /proc/sys/kernel/core_pattern

./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o /home/manos/Desktop/AFL/temp-out/ /home/manos/Desktop/AFL/test-bins/heartbleed



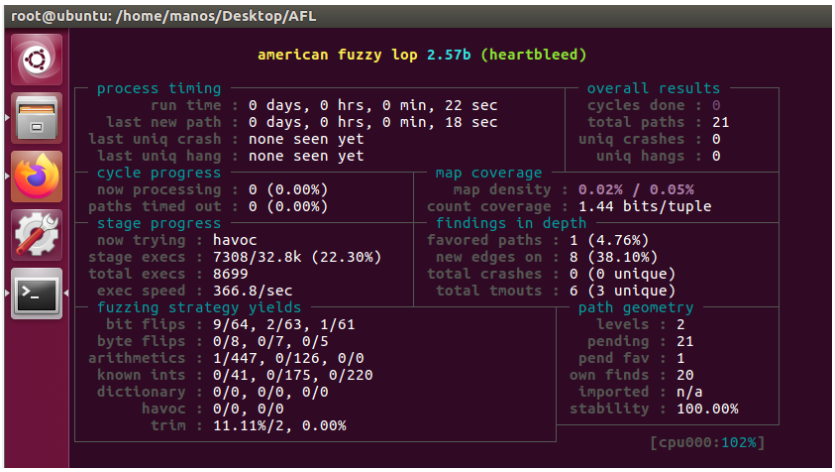
export AFL_SKIP_CPUFREQ=1

sudo su (root) :

echo core >/proc/sys/kernel/core_pattern

./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o /home/manos/Desktop/AFL/temp-out/ /home/manos/Desktop/AFL/test-bins/heartbleed @@

```
+++ Testing aborted by user +++
[+] We're done here. Have a nice day!

root@ubuntu:/home/manos/Desktop/AFL# ./afl-fuzz -i /home/manos/Deskto
/ /home/manos/Desktop/AFL/test-bins/heartbleed @@
afl-fuzz 2.57b by <lcamtuf@google.com>
[+] You have 2 CPU cores and 2 runnable tasks (utilization: 100%).
[*] Checking CPU core loadout...
[+] Found a free CPU core, binding to #0.
[*] Checking core_pattern...
[*] Setting up output directories...
[+] Output directory exists but deemed OK to reuse.
[*] Deleting old session data...
[+] Output dir cleanup successful.
[*] Scanning '/home/manos/Desktop/AFL/temp-in/'...
[+] No auto-generated dictionary tokens to reuse.
[*] Creating hard links for all input files...
[*] Validating target binary...
[*] Attempting dry run with 'id:000000,orig:heartbeat_normal.bin'...
[*] Spinning up the fork server...
[+] All right - fork server is up.
    len = 9, map size = 11, exec speed = 1365 us
[+] All test cases processed.

[+] Here are some useful stats:

    Test case count : 1 favored, 0 variable, 1 total
       Bitmap range : 11 to 11 bits (average: 11.00 bits)
        Exec timing : 1365 to 1365 us (average: 1365 us)

[*] No -t option specified, so I'll use exec timeout of 20 ms.
[+] All set and ready to roll!
```



6. Stop the fuzzer (ctrl C)

7. Compile the heartbleed.c again:

./afl-gcc -m32 -fsanitize=address /home/manos/Desktop/AFL/heartbleed.c -o /home/manos/Desktop/AFL/test-bins/heartbleed-asan

(if this error: usr/include/features.h:367:25: fatal error: sys/cdefs.h: No such file or directory try and install **apt install gcc-multilib)**

Do again: ./afl-gcc -m32 -fsanitize=address heartbleed.c -o test-bins/heartbleed-asan

8. Run fuzzer:

./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o tesmp-out /home/manos/Desktop/AFL/test-bins/heartbleed-asan @@

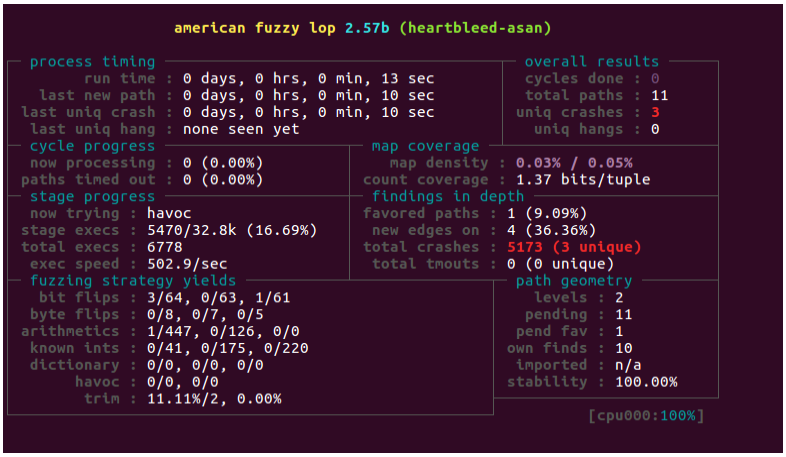
```
manos@ubuntu:~/Desktop/AFL$ ./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o tesmp-out /home/manos/Desktop/AFL/test-bins/heartbleed-asan @@
afl-fuzz 2.57b by <lcamtuf@google.com>
[+] You have 2 CPU cores and 1 runnable tasks (utilization: 50%).
[+] Try parallel jobs - see /usr/local/share/doc/afl/parallel_fuzzing.txt.
[*] Checking CPU core loadout...
[+] Found a free CPU core, binding to #0.
[*] Checking core_pattern...
[*] Setting up output directories...
[*] Scanning '/home/manos/Desktop/AFL/temp-in/'...
[+] No auto-generated dictionary tokens to reuse.
[*] Creating hard links for all input files...
[*] Validating target binary...
[*] Attempting dry run with 'id:000000,orig:heartbeat_normal.bin'...
[*] Spinning up the fork server...

[-] Whoops, the target binary crashed suddenly, before receiving any input
    from the fuzzer! Since it seems to be built with ASAN and you have a
    restrictive memory limit configured, this is expected; please read
    /usr/local/share/doc/afl/notes_for_asan.txt for help.

[-] PROGRAM ABORT : Fork server crashed with signal 6
        Location : init_forkserver(), afl-fuzz.c:2230
```

Run again with -m:

./afl-fuzz -m 600 -i /home/manos/Desktop/AFL/temp-in/ -o tesmp-out /home/manos/Desktop/AFL/test-bins/heartbleed-asan @@

If you get an error saying 600 is too low a memory to run the program, Please try:

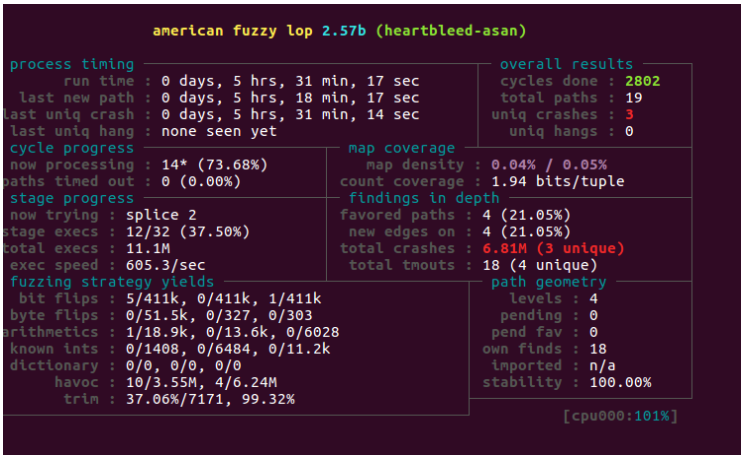
./afl-fuzz -m none -i temp-in/ -o temp-out test-bins/heartbleed-asan @@



9. check the temp-out/crashes directory:

./test-bins/heartbleed-asan <input>

Three unique crashes found:



./test-bins/heartbleed-asan /home/manos/Desktop/AFL/tesmp-out/crashes/id:000000,sig:06,src:000000,op:flip1,pos:1