**COMSM0049 Lab 6**

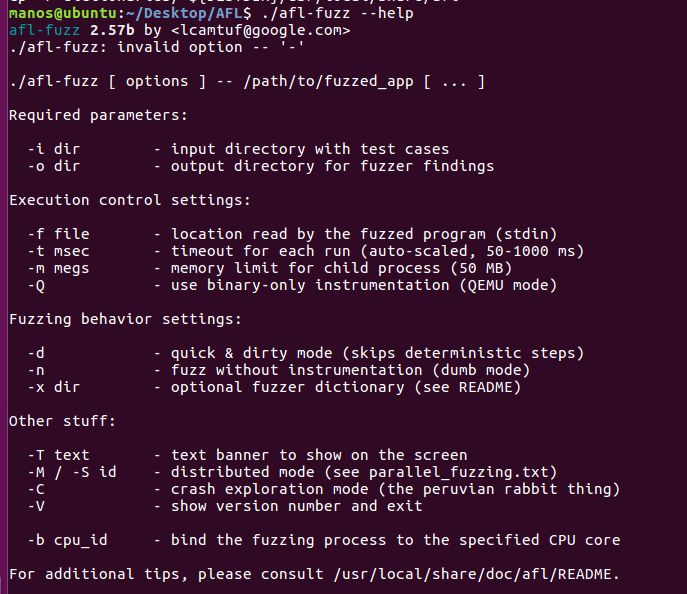
**1. Download and compile AFL:**

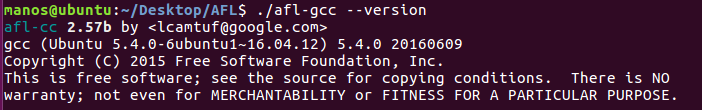
git clone <https://github.com/google/AFL>

cd afl

make && sudo make install

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





**3. create these subdirectories in the root directory:**

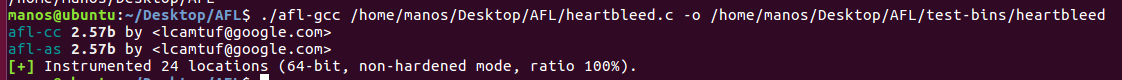
$ mkdir temp-in

$ mkdir temp-out

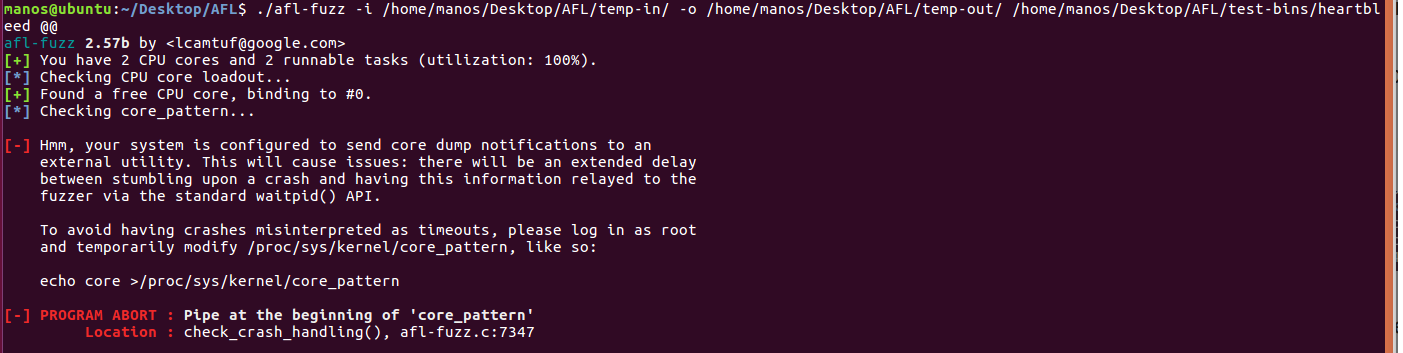
$ mkdir test-bins

3. Move heartbeat\_normal.bin into temp-in:

**4. Compile heartbleed.c**



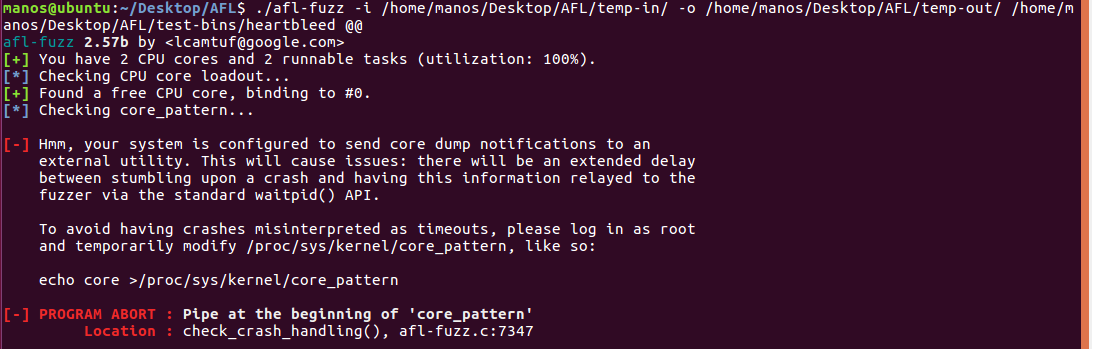
**5. Run AFl fuzzer:** ./afl-fuzz -i /home/manos/Desktop/AFL/temp-in/ -o /home/manos/Desktop/AFL/temp-out/ /home/manos/Desktop/AFL/test-bins/heartbleed @@



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

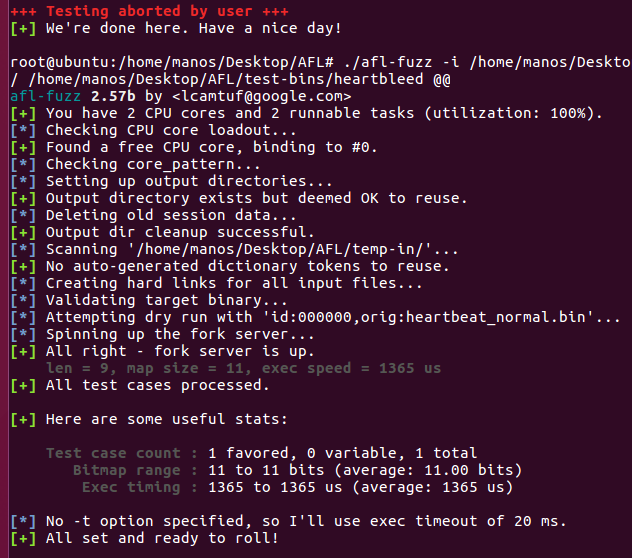


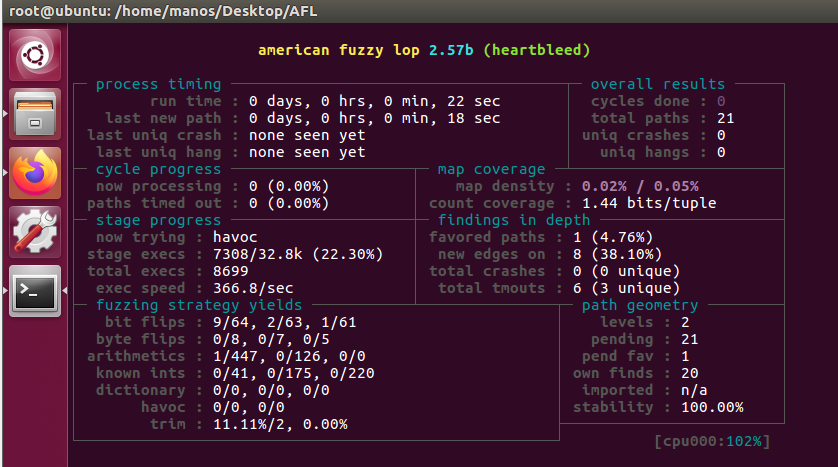
export AFL\_SKIP\_CPUFREQ=1

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 @@





**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 @@

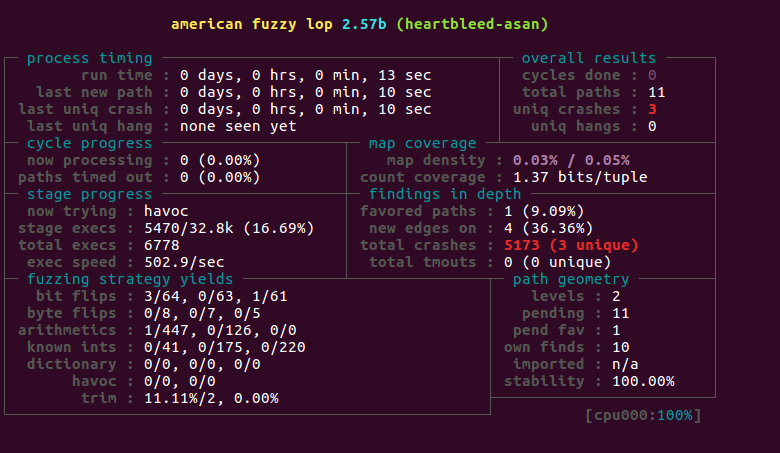


Run again with -m:

./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:

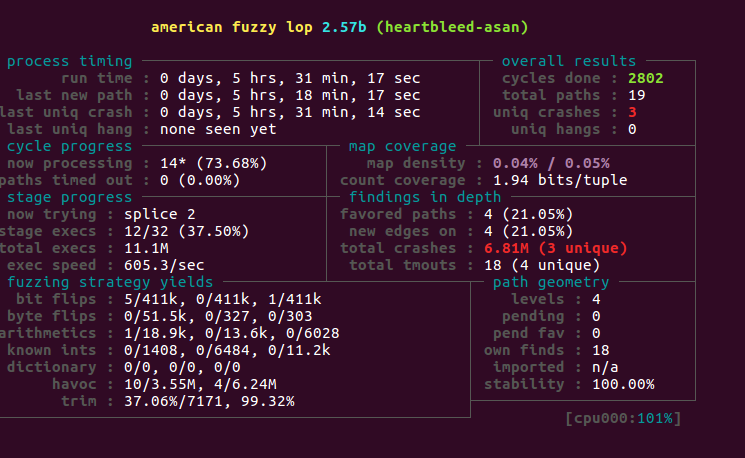
./afl-fuzz -m none -i temp-in/ -o temp-out test-bins/heartbleed-asan @@



**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

