HW3. Symbolic Execution

L091025 清大資工所 熊詩旻

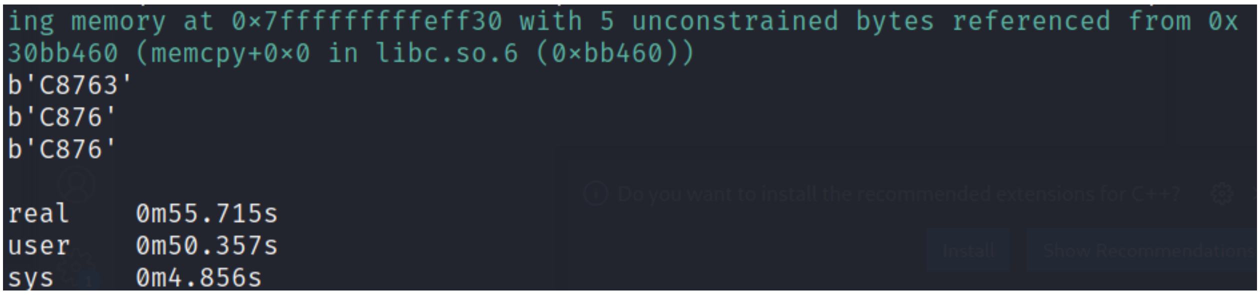
B. Enhanced example

1. Rewrite the script (exploit.py) to speed up its execution. Describe your improvements briefly.

   因為 key 為 5 word

   將 argv1 = claripy.BVS("argv1", 10*8)改寫為 argv1 = claripy.BVS("argv1", 5*8)

2. Run the new script and show your results.

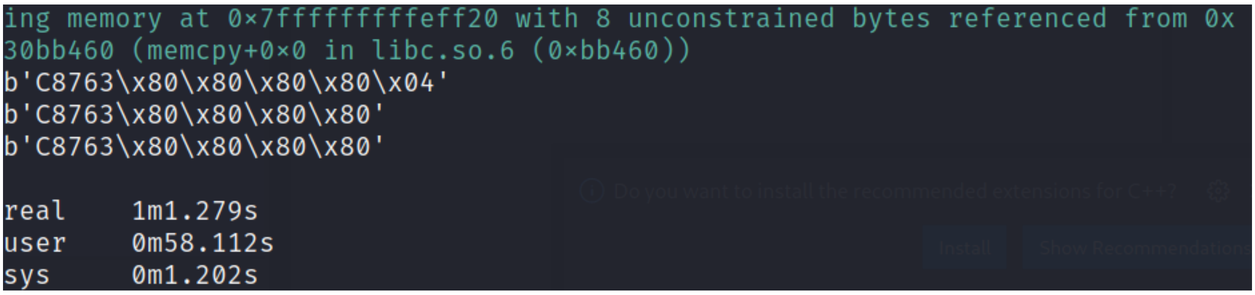


```
ing memory at 0×7fffffffffeff30 with 5 unconstrained bytes referenced from 0x
30bb460 (memcpy+0×0 in libc.so.6 (0×bb460))
b'C8763'
b'C876'
b'C876'

real    0m55.715s
user    0m50.357s
sys     0m4.856s
```

3. Measure and compare the execution time of the new script versus the original script. ($ time python exploit.py)

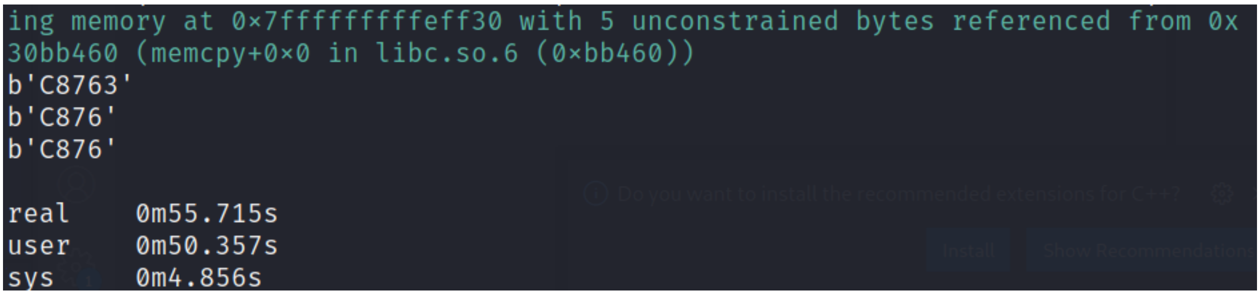
Old:



```
ing memory at 0×7fffffffffeff20 with 8 unconstrained bytes referenced from 0x
30bb460 (memcpy+0×0 in libc.so.6 (0×bb460))
b'C8763\x80\x80\x80\x80\x04'
b'C8763\x80\x80\x80\x80'
b'C8763\x80\x80\x80\x80'

real    1m1.279s
user    0m58.112s
sys     0m1.202s
```

New:



```
ing memory at 0×7fffffffffeff30 with 5 unconstrained bytes referenced from 0x
30bb460 (memcpy+0×0 in libc.so.6 (0×bb460))
b'C8763'
b'C876'
b'C876'

real    0m55.715s
user    0m50.357s
sys     0m4.856s
```