

Sig • Mal

Meeting 8

crackme0x02

```
cs680@cs680-VirtualBox: ~/Documents/compilation_effects
File Edit View Search Terminal Help
cs680@cs680-VirtualBox:~$ cd Documents/compilation_effects/
cs680@cs680-VirtualBox:~/Documents/compilation_effects$ cat *.c
#include <stdio.h>

int main(int argc, char * argv[]) {
    int yoooo;

    printf("Crackme Level 0x02\n");
    printf(">");
    scanf("%d", &yoooo);
    if(yoooo == 0xff) {
        printf("yoooo, sig_fit?\n");
    } else {
        printf("you got no gains, bro\n");
    }
    return 0;
}

Symbol Tree
f _start0
f dispatch
f entry
f exit
f main

080487ed 8b 04 95 MOV EAX,dword ptr [EDX*0x4 + ->discard]
a0 51 3f 08
080487f4 8b 15 40 MOV EDX,dword ptr [stack_temp]
51 1f 08
080487fa 89 10 MOV dword ptr [EAX]>discard,EDX
080487fc 8b 25 60 MOV ESP,dword ptr [->id]
51 3f 08
08048802 c7 05 04 MOV dword ptr [external],exit
2 5f 08
70 82 04 08
0804880c a1 88 51 MOV EAX,[on]
3f 08
08048811 8b 04 85 MOV EAX,dword ptr [EAX*0x4 + ->no_fault]
08 52 5f 08
08048818 50 03 MOV EAX=>no_fault,dword ptr [EAX]

FUNCTION
*****
undefined main()
AL:1 <RETURN>
XREF[1]:
cs680@cs680-VirtualBox:~/Documents/compilation_effects$
3f 08
0804881f ba 1a 88 MOV EDX,0x8804881a
04 88
```

Different Decompilation Methods

- GCC / G++ → GNU C Compiler
- Clang → is a compiler front end for the C, C++, Objective-C and Objective-C++ programming languages, as well as the OpenMP, OpenCL, RenderScript, CUDA and HIP frameworks. It uses the LLVM compiler infrastructure as its back end and has been part of the LLVM release cycle since LLVM 2.6
- MOVCC → movfuscator for reversing
- Distcc → tool for speeding up compilation of source code by using distributed computing over a computer network. With the right configuration, distcc can dramatically reduce a project's compilation time

Application for Fuzzy Hashing

- Let's use our boy, ssdeep

```
>> ssdeep -pb *
```

```
cs680@cs680-VirtualBox: ~/Documents/compilation_effects
File Edit View Search Terminal Help
cs680@cs680-VirtualBox:~/Documents/compilation_effects$ ls
ko.c ko_clang ko_distcc ko_gcc ko_movcc
cs680@cs680-VirtualBox:~/Documents/compilation_effects$ ssdeep -pb
ko_distcc matches ko_gcc (100)
ko_gcc matches ko_distcc (100)
cs680@cs680-VirtualBox:~/Documents/compilation_effects$
```

Compilation Methods (CLICK ME)

[GCC](#)

[CLANG](#)

[MOVCC](#)

[DISTCC](#)

Hypotheticals Hacks

- ServiceMain
- + In software, normally you write functions names that provide useful information

So your 'program' doesn't run so then Hypothetically...

Hypotheticals Hacks

- ServiceMain

- + In software, normally you write functions names that provide useful information

→ Check Microsoft Documentation → Learn that in order to run a program as a service, define a 'ServiceMain' function

→ The presence of an exported function called 'ServiceMain' tells you that your software runs as part of a service

LIVE DEMO TIME