

Password Cracking

- 1) First to hack the program I found where the program was going and placed a break point in the check_cdkey function. From there I followed the program until I found a point where it jumped to line 0x08048640 if there was condition met. So, I set a break point at that memory address and ran the program again. This time when I was in the check_cdkey function I forced a return of 1 and noticed that I hit the break point at that memory address which then proceeded to return a fortune.

```
— Output/messages —
Breakpoint 2, 0x08048640 in main ()
— Assembly —
0x08048636 main+86 push    $0x1
0x08048638 main+88 call    0x804ad70 <exit>
0x0804863d main+93 lea     0x0(%esi),%esi
0x08048640 main+96 call    0x8048290 <get_quotes_file>
0x08048645 main+101 mov     %eax,%eax
0x08048647 main+103 mov     %eax,-0x10c(%ebp)
0x0804864d main+109 cmpl    $0x0,-0x10c(%ebp)
— Expressions —
— History —
— Memory —
— Registers —
eax 0x00000001   ecx 0xfbad2288   edx 0x00000000   ebx 0x080954c0
es 0x0000002b   fs 0x00000000   gs 0x00000000
— Source —
— Stack —
[0] from 0x08048640 in main+96
(no arguments)
— Threads —
[1] id 2939 name fortune_static from 0x08048640 in main+96
>>> █
```

```
— Output/messages —
Your fortune:

"A wizard cannot do everything; a fact most magicians are reticent to admit,
let alone discuss with prospective clients. Still, the fact remains that
there are certain objects, and people, that are, for one reason or another,
completely immune to any direct magical spell. It is for this group of
beings that the magician learns the subtleties of using indirect spells.
It also does no harm, in dealing with these matters, to carry a large club
near your person at all times."

-- The Teachings of Ebenezum, Volume VIII

[Inferior 1 (process 2938) exited with code 053]
>>> █
```

- 2) To get the program to bypass the cdkey mechanism I broke the program down into assembly and found the portion where the function was located. The function would jump to two different lines returning 1 or 0. I modified the return 0 to also return 1. This made it so that it would always return 1 and hit that line of code at 0x08048640 and print a fortune.
- 3) Following the program to where I got the fortune previously it called the get_quotes_file function. Following the program into that function I noticed it called another function called print_fortune. Going into this function the first step was a pointer to the location of the fortunes. Setting breakpoint there and calling print on that memory location revealed the remaining fortunes.