Keith's Annoying Friend (300)

Uday Shankar

The best way to analyze this problem is to take a look at how exactly I made it. First, I wrote a simple C program whose output you can see by running the program on a Linux machine (though actually running the program doesn't help at all). Then, to the produced binary, I injected an additional section called `.caesar_secret`. This section had flags on it to prevent its actual loading into memory, which explains why debuggers were generally useless or at least not the preferred tool. Instead, the best way to do this problem was to disassemble the section and look directly at the hex data. On Linux, one would perhaps do this using the command `objdump -sj .caesar_secret annoy`. The data inside this extra section is simply the caesar-shifted flag. A common pitfall was including the byte offsets printed at the beginning of each line by `objdump` in the data to be caesar shifted - this yields extraneous characters in the flag.