Cyber forensics HW1 Report

tags: `class`

1. How My Pintool Works

I identified the critical branches by address in the code and changed the values of some registers so the result of the cmp insturctions would become true, forcing the program to execute the originally unexecuted part.

2. Triggering conditions

`cmp eax, 0x806ea`, `cmp eax, 0xbfebfbff`, `cmp eax, 0xa0`, `cmp eax, 0x19`, `cmp al, 0xa`

The first condition is something about CPU information and time.

3. Suspicous Activity

The program tries to open `/etc/passwd` and write it to `/tmp/leak`

4. Handleing the packer

I packed a hello world program and compare it with the original code by tracing syscalls and instructions. I found that the original code starts after a syscall number 11, so I tried to find it in the memory trace output file. Finally I found the syscall was at 0x40000c and that after that was where the original code starts.

5. How I alanylized the sample

Having found where the main function starts, I tried to find all the critical cmp and jump instructions that control the program flow.