

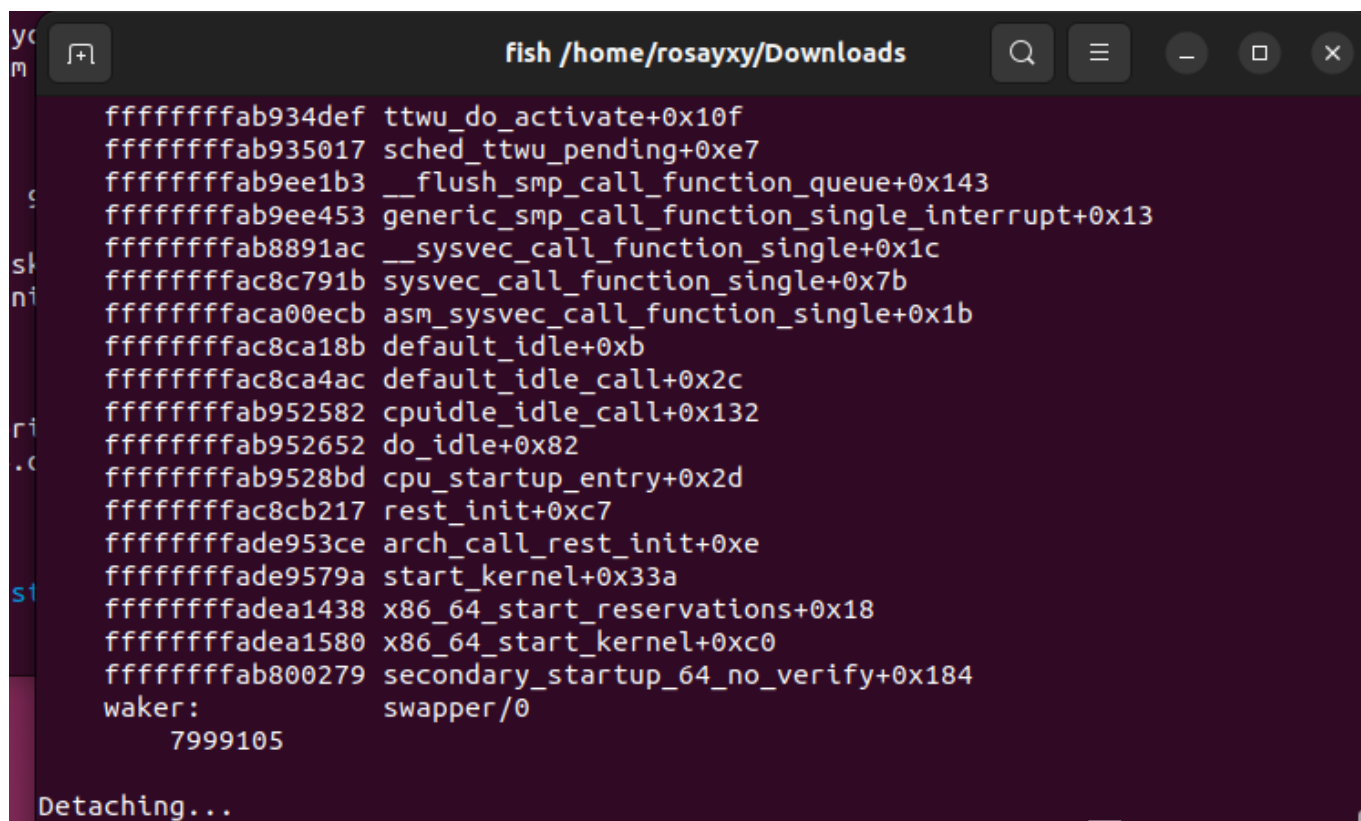
操作系统第九次作业

问题一

在 wsl 和 hyper-v 22.04 虚拟机里面直接 `sudo apt-get install bpfcc-tools linux-headers-$(uname -r)` 都会出现报错

简单搜了一下 解决方法是从 source rebuild

然后 rebuild 的时候会报错大概是找不到符号的问题，怀疑还是找到了旧的 bpfcc-tools，验证为 `dpkg -S libbcc.so.0` 看到有两个，分别装在 /usr/bin 和 /usr/local 下面，所以 `sudo apt remove libbpfcc` 一波然后 `sudo make install` 之后就正常了



```
fish /home/rosayxy/Downloads
fffffffab934def ttwu_do_activate+0x10f
fffffffab935017 sched_ttwu_pending+0xe7
fffffffab9ee1b3 __flush_smp_call_function_queue+0x143
fffffffab9ee453 generic_smp_call_function_single_interrupt+0x13
fffffffab8891ac __sysvec_call_function_single+0x1c
fffffffac8c791b sysvec_call_function_single+0x7b
fffffffac8ca0ecb asm_sysvec_call_function_single+0x1b
fffffffac8ca18b default_idle+0xb
fffffffac8ca4ac default_idle_call+0x2c
fffffffab952582 cpuidle_idle_call+0x132
fffffffab952652 do_idle+0x82
fffffffab9528bd cpu_startup_entry+0x2d
fffffffac8cb217 rest_init+0xc7
fffffffade953ce arch_call_rest_init+0xe
fffffffade9579a start_kernel+0x33a
fffffffadea1438 x86_64_start_reservations+0x18
fffffffadea1580 x86_64_start_kernel+0xc0
fffffffab800279 secondary_startup_64_no_verify+0x184
waker:
7999105 swapper/0
Detaching...
```

问题三

[seccomp-tools](#) 由 bpf 实现

以及近日对 bpf 的原理 & 攻击流程进行一些研究并写博客如下：

<https://rosayxy.github.io/ebpf-pwn-intro/>