1. 修复内核模块

- 对`UAF`漏洞进行修复，操作即在`kfree`之后，添加对于指针的置空操作；
- 对空指针引用漏洞进行修复，操作即在使用指针之前判断该指针是否为空：

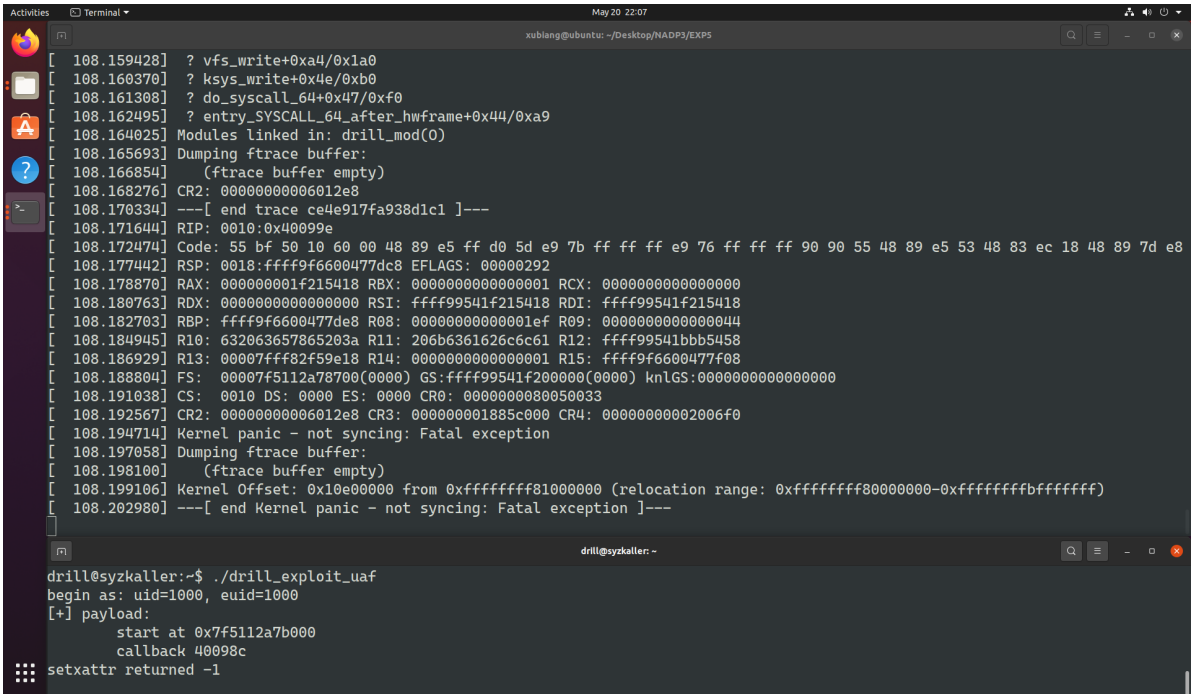
```
static int drill_act_exec(long act) {
    int ret = 0;

    switch (act) {
        case DRILL_ACT_ALLOC:
            ...

        case DRILL_ACT_CALLBACK:
            pr_notice("drill: exec callback %lx for item %lx\n",
                      (unsigned long)drill.item->callback,
                      (unsigned long)drill.item);
            if (drill.item) {
                drill.item->callback();  // Add check by XBA, GOOD GOOD GOOD
            }
            // drill.item->callback(); // No check, BAD BAD BAD
            break;

        case DRILL_ACT_FREE:
            pr_notice("drill: free item at %lx\n",
                      (unsigned long)drill.item);
            kfree(drill.item);
            drill.item = NULL;                          // Add by XBA
            pr_notice("drill: set item ptr to NULL\n");  // Add by XBA
            break;

        case DRILL_ACT_RESET:
            ...

        default:
            ...
    }

    return ret;
}
```

2. 开启SMAP

- 开启防御措施`SMAP`（`Supervisor Mode Access Prevention`）来禁止从内核空间访问用户空间：

```
# 使用该命令启动QEMU虚拟机，使用-cpu kvm64,smap开启smap
qemu-system-x86_64 \
-cpu kvm64,smap \
-kernel linux-5.0-rc1/arch/x86/boot/bzImage \
-append "console=ttyS0 root=/dev/sda debug earlyprintk=serial slub_debug=QUZ
pti=off oops=panic ftrace_dump_on_oops nokaslr"\
-hda wheezy.img \
-net user,hostfwd=tcp::10021-:22 -net nic \
-nographic -m 512M -smp 2 \
-pidfile vm.pid 2>&1 | tee vm.log
```

- 开启 SMAP 后使用 drill_exploit_uaf 进行攻击失败：



- 开启`SMAP`后使用`drill_exploit_nullderef进行攻击失败：