

# Kernel Pwn Cheat Sheet

## Kernel Version

```
commit 09688c0166e76ce2fb85e86b9d99be8b0084cdf9 (HEAD -> master, tag: v5.17-rc8,
origin/master, origin/HEAD)
Author: Linus Torvalds <torvalds@linux-foundation.org>
Date: Sun Mar 13 13:23:37 2022 -0700
```

Linux 5.17-rc8

## Rturn to usermode

- [swapgs\\_restore\\_regs\\_and\\_return\\_to\\_usermode](#)

## Structures

structure	slab	flag	memo
shm_file_data	32	GFP_KERNEL	
seq_operations	32	GFP_KERNEL_ACCOUNT	/proc/self/stat
msg_msg	64 ~ 1024	GFP_KERNEL_ACCOUNT	
msg_msgseg	8 ~ 1024	GFP_KERNEL_ACCOUNT	
subprocess_info	128	GFP_KERNEL	socket(22, AF_INET, 0);
timerfd_ctx	256	GFP_KERNEL	
tty_struct	1024	GFP_KERNEL	/dev/ptmx
pipe_buffer	1024	GFP_KERNEL_ACCOUNT	
setxattr	8 ~	GFP_KERNEL	

### shm file data

- [do\\_shmat](#)

### seq\_operations

- [proc\\_stat\\_init](#)
  - [stat\\_proc\\_ops](#)
- [stat\\_open](#)
  - [single\\_open\\_size](#)
    - [single\\_open](#)
- [seq\\_read\\_iter](#)
  - m->op->start

### msg\_msg / msg\_msgseg

- [do\\_msgsnd](#)
  - [load\\_msg](#)
    - [alloc\\_msg](#)
- [do\\_msgrcv](#)
  - `#define MSG_COPY 040000`

## **subprocess\_info**

- [\\_\\_sys\\_socket](#)
  - [sock\\_create](#)
    - [\\_\\_sock\\_create](#)
      - [\\_\\_request\\_module](#)
      - [call\\_modprobe](#)
      - [call\\_usermodehelper\\_setup](#)

## **timerfd\_ctx**

- [timerfd\\_create](#)
- [timerfd\\_release](#)
  - `kfree_rcu`

## **tty\_struct**

- [unix98\\_pty\\_init](#)
  - [tty\\_default\\_fops](#)
    - [tty\\_fops](#)
- [ptmx\\_open](#)
  - [tty\\_init\\_dev](#)
    - [alloc\\_tty\\_struct](#)
- [tty\\_ioctl](#)
  - [tty\\_paranoia\\_check](#)
    - `#define TTY_MAGIC 0x5401`
  - [tty\\_pair\\_get\\_tty](#)
  - `tty->ops->ioctl`

## **pipe\_buffer**

- [do\\_pipe2](#)
  - [do\\_pipe\\_flags](#)
    - [create\\_pipe\\_files](#)
      - [get\\_pipe\\_inode](#)
        - [alloc\\_pipe\\_info](#)
    - [pipefifo\\_fops](#)
- [pipe\\_release](#)
  - [put\\_pipe\\_info](#)
    - [free\\_pipe\\_info](#)
    - [pipe\\_buf\\_release](#)
      - `ops->release`

**setxattr**

- [setxattr](#)

**Variables**

variable	path
modprobe_path	/proc/sys/kernel/modprobe
core_pattern	/proc/sys/kernel/core_pattern

**modprobe\_path**

- do\_execve
  - do\_execveat\_common
    - bprm\_execve
      - exec\_binprm
        - [search\\_binary\\_handler](#)
          - [\\_\\_request\\_module](#)
            - [call\\_modprobe](#)
              - call\_usermodehelper\_setup
              - call\_usermodehelper\_exec

**core\_pattern**

- [do\\_coredump](#)
  - [format\\_corename](#)
  - call\_usermodehelper\_setup
  - call\_usermodehelper\_exec