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