Dirty COW 漏洞

版权所有 © 2017 作者：杜文亮，保留所有权利。
允许个人使用。利用这些问题只有当作者的书被采用作为该课程的教科书时，该课程才被授予。所有其他用途必须征得作者同意。

S8.1. 某文件内容为 "Hello World"，整个文件经 mmap() 映射后，起始地址保存在 map。下列 printf() 会输出什么？

```
char *addr = (char *)map;
printf("%s\n", map +6);
```

S8.2. fork() 创建的子进程具有父进程地址空间的逻辑副本，但系统通常不会在创建瞬间复制所有物理内存。实际复制何时发生？

S8.3. 进程使用 MAP_PRIVATE 把文件映射到内存，布局如图 1。（1）进程向地址 0x5100 写入时会发生什么？（2）Dirty COW 竞态发生在内核写入路径中，具体竞争在哪里？（3）攻击者如何利用该竞态？

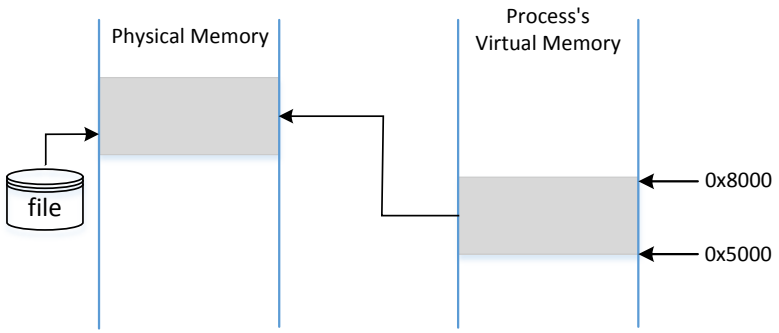

图 1: 问题图 S8.3.

S8.4. 用户 seed 对 /home/seed/zzz 有读写权限。由 seed 执行下列代码，会修改磁盘上的文件内容吗？

```
int f=open("/home/seed/zzz", O_RDWR);
fstat(f, &st);
// Map the entire file to memory
map=mmap(NULL, st.st_size, PROT_READ|PROT_WRITE,
                           MAP_PRIVATE, f, 0);
memcpy(map, "new content", strlen("new content"));
```

S8.5. Dirty COW 攻击中能否用两个独立进程代替同一进程内的两个线程？

S8.6. 本章通过 Dirty COW 修改 `/etc/passwd` 并取得 root 权限。请再举两个可通过篡改而实现提权的文件。

S8.7. 若用 `MAP_PRIVATE` 把只读文件映射到内存，再用 `memcpy()` 向映射写入，会触发写时复制吗？

S8.8. ★ ★
为什么不能指望 `memcpy()` 自动为只读私有映射触发写时复制，从而得到可写副本？