

**Syscalls**

***Objective: In this lab you will run a LKM called “unlinker”. The LKM will intercept the syscall for the unlink() function and prevent any user, including root, from unlinking a file.***

***Reference:*** LKI/labs/Lab12

1. The unlinker LKM should intercept and block unlink attempts:





1. First, get the address of your sys\_call\_table form the System.map.
2. Next change the sys\_call\_table to read/write using the code provided.
3. Save the address of the original unlink function before overwriting it with your own (that way after you unload your module you restore the unlink function).