

Sistemas Operacionais

Rodrigo Rubira Branco rodrigo@kernelhacking.com rodrigo@fgp.com.br

Chamadas ao Sistema (modo usuario)

```
#include <sys/types.h>
#include <unistd.h>
main(){
    if (setuid(1001)) {
               perror("\n Mudando de usuario\n");
               exit(-1);
     printf("\n UserID: %d\n",getuid());
    if ( chdir("/teste") ) {
               perror("\n Mudando para o diretorio /teste\n");
               exit(-1);
    printf("\n Tive permissoes\n");
```



Chamadas ao Sistema (modo usuario)

```
#include <sys/syscall.h>
/* SYS_exit = NR_exit = 1 (definido em
/usr/include/asm-i386/unistd.h */
#define sys_mycall(x) syscall(SYS_exit,x);
main()
   sys_mycall(10);
```



Chamadas ao Sistema (modo usuario)

```
execve("./syscall", ["./syscall"], [/* 19 vars */]) = 0
uname({sys="Linux", node="notedell", ...}) = 0
brk(0) = 0x8049600
```

munmap(0x40017000, 82007) = 0

$$=$$
?





FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco rodrigo@kernelhacking.com