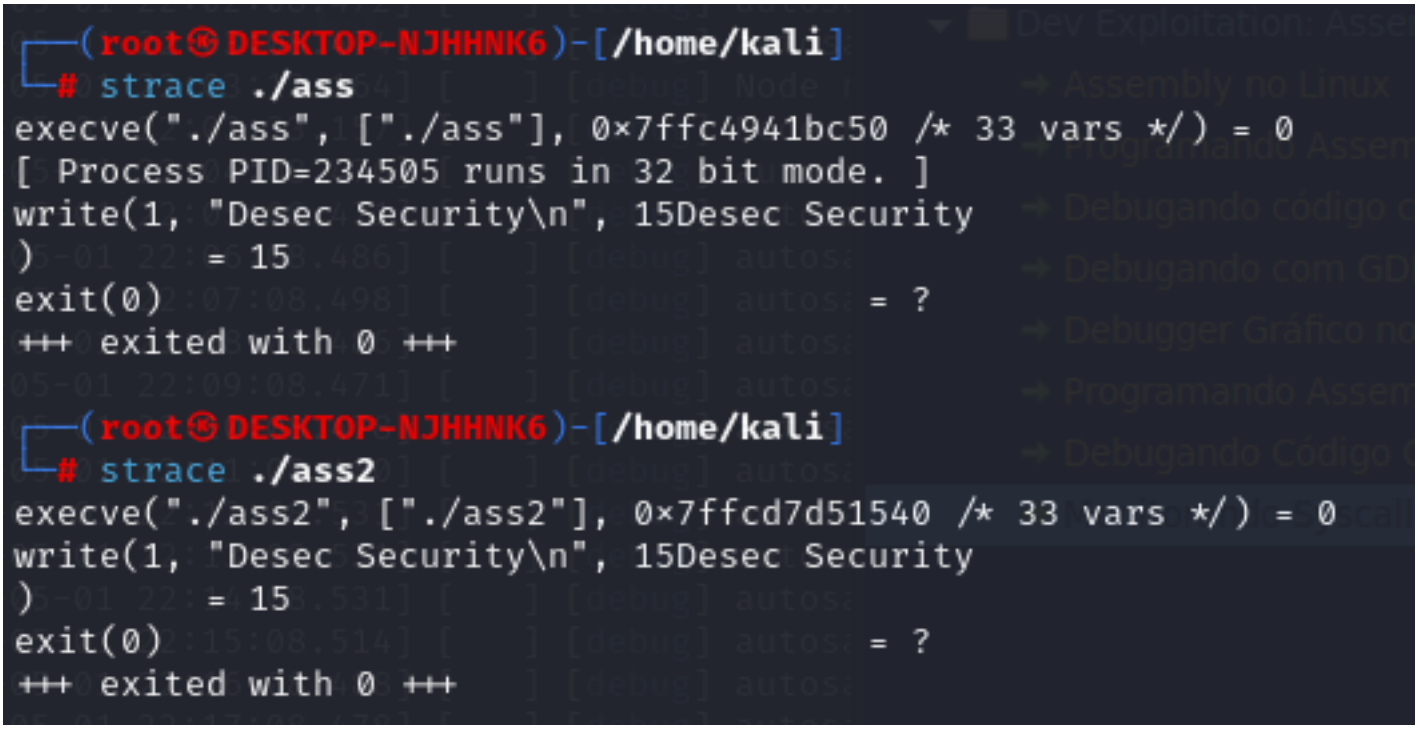
Monitorando Syscalls

+ O strace intercepta e registra as chamadas de sistemas que determinado programa faz

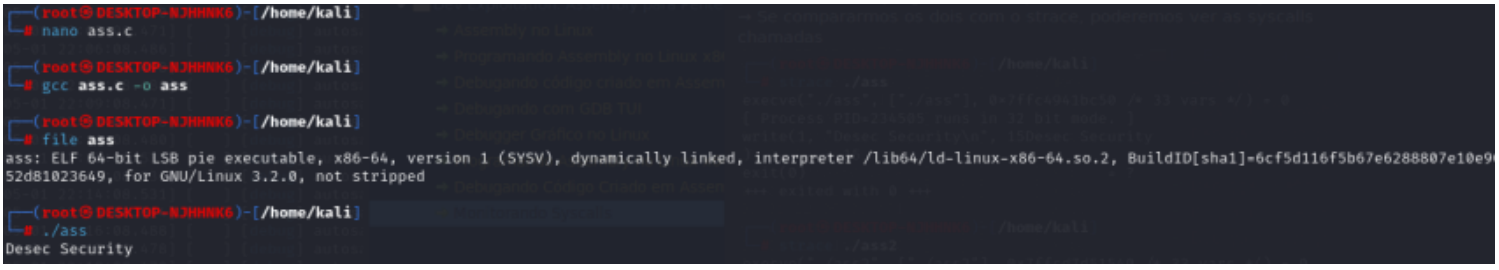
```
--------------------------------ass.c-----------------------------------
#include <stdio.h>

int main (){
	printf("Desec Security\n");
	return 0;
}
------------------------------------------------------------------------
```

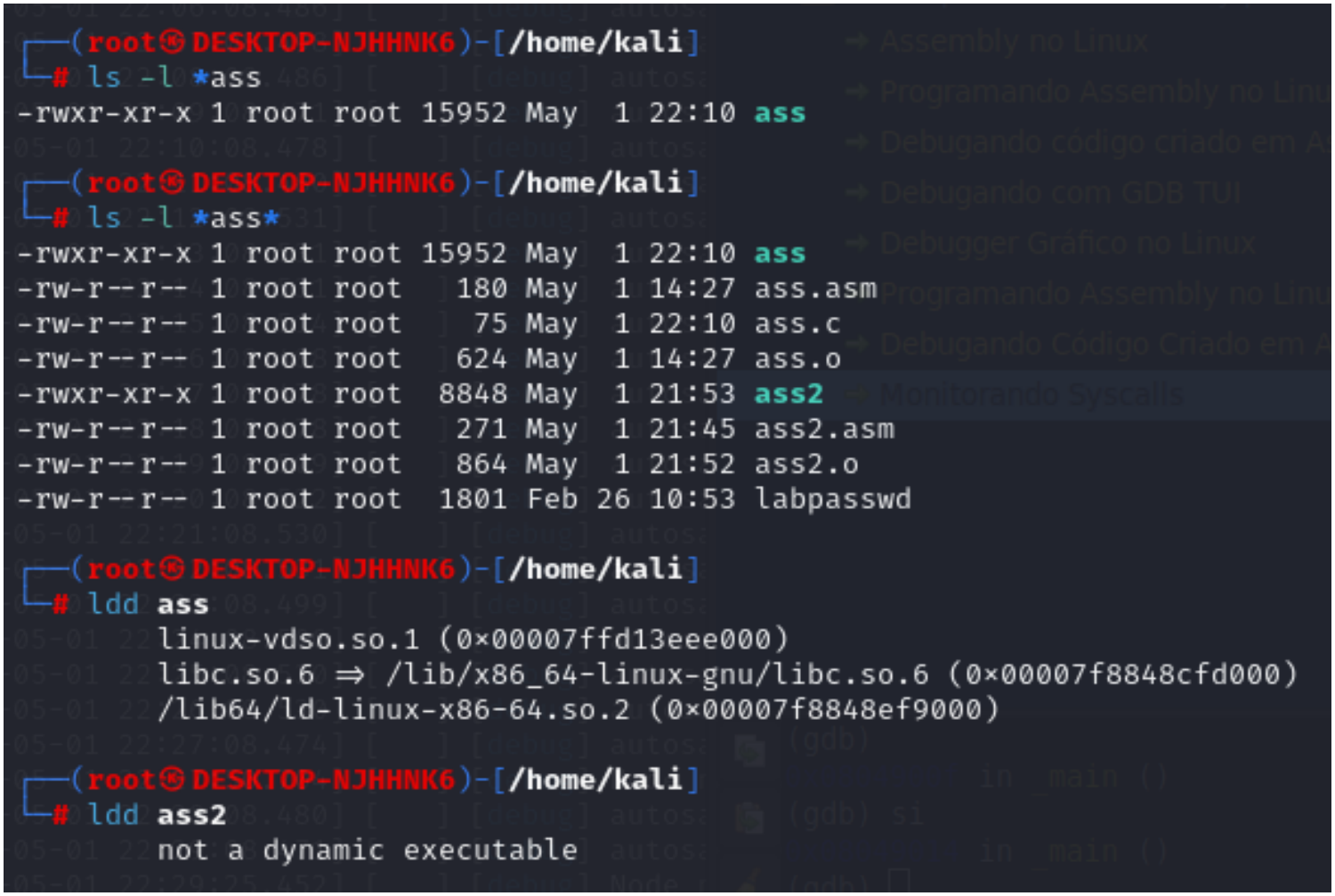
→ Montamos um programa em C que executa as mesmas funções
→ Se compararmos os dois com o strace, poderemos ver as syscalls chamadas



→ Ao monstarmos o programa em c que faz a mesma coisa, vemos que ele será do formato 64-bits



→ Se compararmos os tamanhos, vemos que os programas em Assembly são bem menores
→ Além disso, os em c se usam de libs para se comunicar com a máquina, enquanto o outro já comunica diretamente



→ Se quisermos debugar o código em c veremos o quão grande ele é

```
strace ./ass
```

```
objdump -d -M intel ass
```

```
ltrace ./ass
```

```
ltrace -S ./ass
```