

```
mov %esp,%ecx
and $0xfffff0,%esp
push %eax
push %esp
push %edx
push $0x80486c0
push $0x80486d0
push %ecx
push %esi
push $0x8048510
call 0x08048414
```

```
vma: 0x08048414
jmp *0x80498d4
```

\_\_libc\_start\_main

0x080484a1

```
vma: 0x08048662
add %eax,-0x2074(%ebp)
jmp 0x08048600
```

```
vma: 0x08048600
cmp $0x1fff,%edi
mov $0x2000,%esi
ja 0x0804860f
```

```
vma: 0x0804865c
lea 0x0(%esi,%eiz,1),%esi
je 0x0804866a
```

```
vma: 0x080486c5
lea 0x0(%esi,%eiz,1),%esi
lea 0x0(%edi,%eiz,1),%edi
push %ebp
mov %esp,%ebp
push %edi
push %esi
push %ebx
call 0x0804872a
```

```
vma: 0x0804872a
mov (%esp),%ebx
ret
```

```
vma: 0x080486db
add $0x11e1,%ebx
sub $0xc,%esp
call 0x080483a4
```

```
vma: 0x080483a4
push %ebp
mov %esp,%ebp
push %ebx
sub $0x4,%esp
call 0x080483b0
```

```
vma: 0x080486e9
lea -0xe8(%ebx),%edi
lea -0xe8(%ebx),%eax
sub %eax,%edi
sar $0x2,%edi
test %edi,%edi
je 0x08048722
```

```
vma: 0x080483e0
add %al,(%eax)
add %al,(%eax)
jmp *0x80498c8
```

mmap

stderr

\_\_gmon\_start\_\_