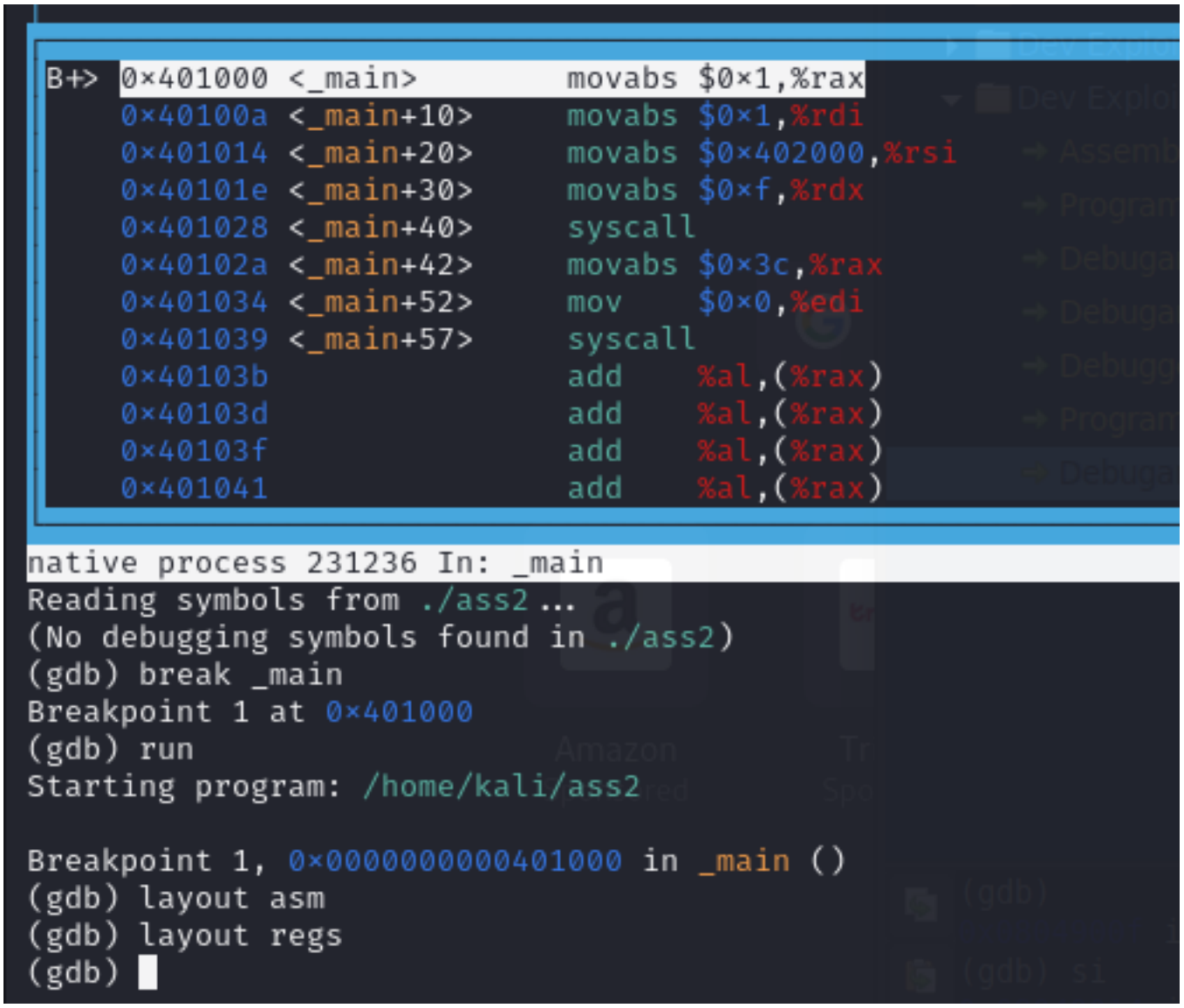
Debugando Código Criado em Assembly x64

```
(gdb) disas
Dump of assembler code for function _main:
⇒ 0x0000000000401000 <+0>:     movabs $0x1,%rax
   0x000000000040100a <+10>:    movabs $0x1,%rdi
   0x0000000000401014 <+20>:    movabs $0x402000,%rsi
   0x000000000040101e <+30>:    movabs $0xf,%rdx
   0x0000000000401028 <+40>:    syscall
   0x000000000040102a <+42>:    movabs $0x3c,%rax
   0x0000000000401034 <+52>:    mov    $0x0,%edi
   0x0000000000401039 <+57>:    syscall
End of assembler dump.
(gdb) set disassembly-flavor intel
(gdb) disas
Dump of assembler code for function _main:
⇒ 0x0000000000401000 <+0>:     movabs rax,0x1
   0x000000000040100a <+10>:    movabs rdi,0x1
   0x0000000000401014 <+20>:    movabs rsi,0x402000
   0x000000000040101e <+30>:    movabs rdx,0xf
   0x0000000000401028 <+40>:    syscall
   0x000000000040102a <+42>:    movabs rax,0x3c
   0x0000000000401034 <+52>:    mov    edi,0x0
   0x0000000000401039 <+57>:    syscall
End of assembler dump.
```

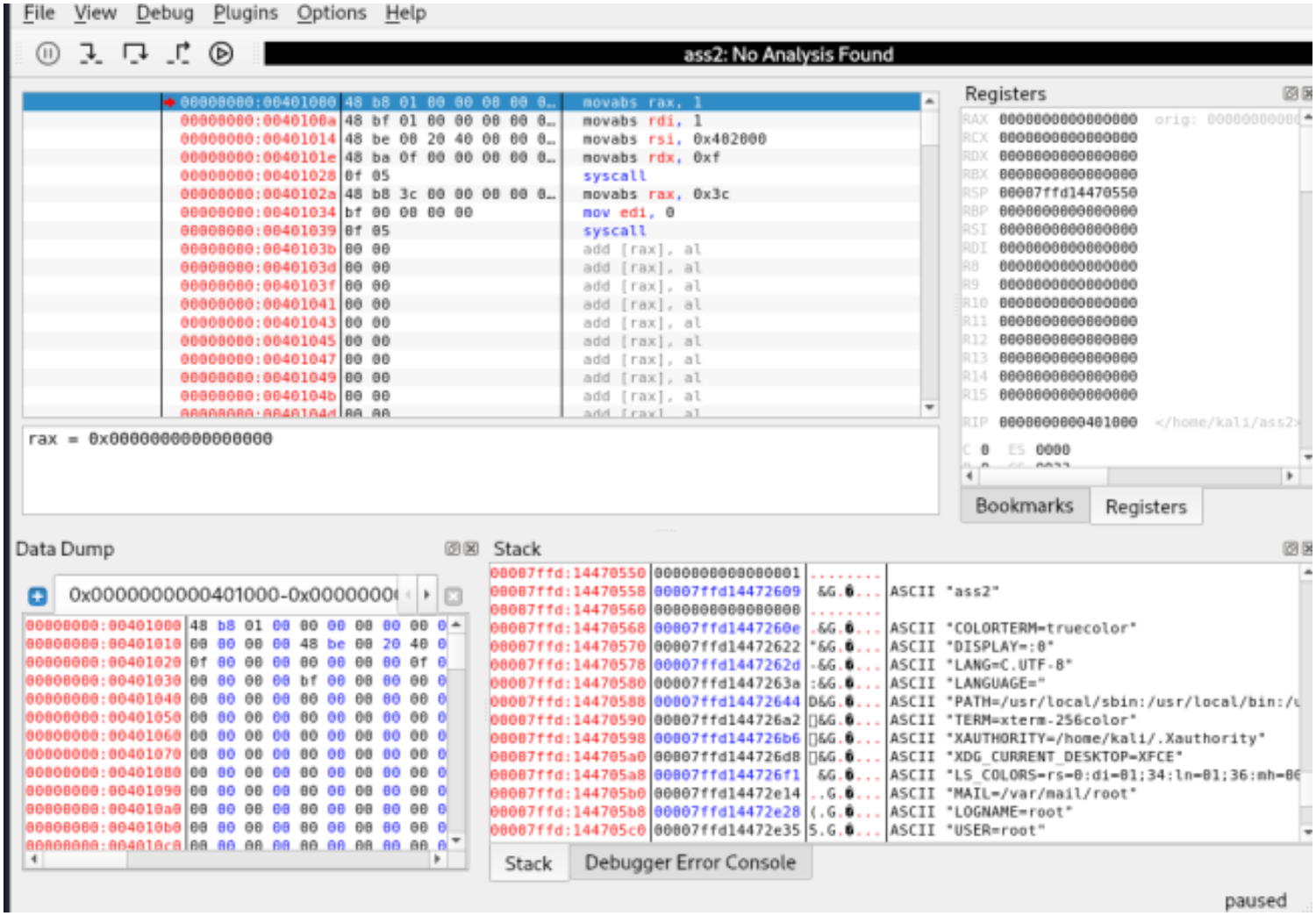
```
(gdb) si
0x000000000040100a in _main ()
(gdb) i r
rax            0x1                 1
rbx            0x0                 0
rcx            0x0                 0
rdx            0x0                 0
rsi            0x0                 0
rdi            0x0                 0
rbp            0x0                 0x0
rsp            0x7fffffffe310      0x7fffffffe310
r8             0x0                 0
r9             0x0                 0
r10            0x0                 0
r11            0x0                 0
r12            0x0                 0
r13            0x0                 0
r14            0x0                 0
r15            0x0                 0
rip            0x40100a            0x40100a <_main+10
eflags         0x202               [ IF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
(gdb) disas
Dump of assembler code for function _main:
   0x0000000000401000 <+0>:     movabs rax,0x1
⇒  0x000000000040100a <+10>:    movabs rdi,0x1
   0x0000000000401014 <+20>:    movabs rsi,0x402000
   0x000000000040101e <+30>:    movabs rdx,0xf
   0x0000000000401028 <+40>:    syscall
   0x000000000040102a <+42>:    movabs rax,0x3c
   0x0000000000401034 <+52>:    mov    edi,0x0
   0x0000000000401039 <+57>:    syscall
End of assembler dump.
```

```
(gdb) x/s 0x402000
0x402000:       "Desec Security\n"
```

```
gdb -q ./ass2 -tui
```


B+> 0×401000 <_main> movabs $0×1,%rax
0×40100a <_main+10> movabs $0×1,%rdi
0×401014 <_main+20> movabs $0×402000,%rsi
0×40101e <_main+30> movabs $0×f,%rdx
0×401028 <_main+40> syscall
0×40102a <_main+42> movabs $0×3c,%rax
0×401034 <_main+52> mov $0×0,%edi
0×401039 <_main+57> syscall
0×40103b add %al,(%rax)
0×40103d add %al,(%rax)
0×40103f add %al,(%rax)
0×401041 add %al,(%rax)
native process 231236 In: _main
Reading symbols from ./ass2...
(No debugging symbols found in ./ass2)
(gdb) break _main
Breakpoint 1 at 0×401000
(gdb) run
Starting program: /home/kali/ass2
Breakpoint 1, 0×0000000000401000 in _main ()
(gdb) layout asm
(gdb) layout regs
(gdb)

```
edb --run ass2
```


File View Debug Plugins Options Help
ass2: No Analysis Found
00000000:00401000 48 b8 01 00 00 00 00 0… movabs rax, 1
00000000:0040100a 48 bf 01 00 00 00 00 0… movabs rdi, 1
00000000:00401014 48 be 00 20 40 00 00 0… movabs rsi, 0x402000
00000000:0040101e 48 ba 0f 00 00 00 00 0… movabs rdx, 0xf
00000000:00401028 0f 05 syscall
00000000:0040102a 48 b8 3c 00 00 00 00 0… movabs rax, 0x3c
00000000:00401034 bf 00 00 00 00 mov edi, 0
00000000:00401039 0f 05 syscall
00000000:0040103b 00 00 add [rax], al
00000000:0040103d 00 00 add [rax], al
00000000:0040103f 00 00 add [rax], al
00000000:00401041 00 00 add [rax], al
00000000:00401043 00 00 add [rax], al
00000000:00401045 00 00 add [rax], al
00000000:00401047 00 00 add [rax], al
00000000:00401049 00 00 add [rax], al
00000000:0040104b 00 00 add [rax], al
rax = 0x0000000000000000
Registers
RAX 0000000000000000
RCX 0000000000000000
RDX 0000000000000000
RBX 0000000000000000
RSP 00007ffd14470550
RBP 0000000000000000
RSI 0000000000000000
RDI 0000000000000000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 0000000000401000
Bookmarks
Registers
Data Dump
0x0000000000401000-0x0000000
Stack
00007ffd:14470550 0000000000000001
00007ffd:14470558 00007ffd14472609 ASCII "ass2"
00007ffd:14470560 0000000000000000
00007ffd:14470568 00007ffd1447260e ASCII "COLORTERM=truecolor"
00007ffd:14470570 00007ffd14472622 ASCII "DISPLAY=:0"
00007ffd:14470578 00007ffd1447262d ASCII "LANG=C.UTF-8"
00007ffd:14470580 00007ffd1447263a ASCII "LANGUAGE="
00007ffd:14470588 00007ffd14472644 ASCII "PATH=/usr/local/sbin:/usr/local/bin:/
00007ffd:14470590 00007ffd144726a2 ASCII "TERM=xterm-256color"
00007ffd:14470598 00007ffd144726b6 ASCII "XAUTHORITY=/home/kali/.Xauthority"
00007ffd:144705a0 00007ffd144726d8 ASCII "XDG_CURRENT_DESKTOP=XFCE"
00007ffd:144705a8 00007ffd144726f1 ASCII "LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00
00007ffd:144705b0 00007ffd14472e14 ASCII "MAIL=/var/mail/root"
00007ffd:144705b8 00007ffd14472e28 ASCII "LOGNAME=root"
00007ffd:144705c0 00007ffd14472e35 ASCII "USER=root"
Stack
Debugger Error Console
paused