

Debugando Código Criado em Assembly x64

```
(root@DESKTOP-NJHHNK6)-[/home/kali] autos:
# gdb -q ./ass2:02.343] [      ] [debug] Node: i ▶ ✖ SEK
Reading symbols from ./ass2 ... [debug] Node: i ▶ ✖ SEK
(No debugging symbols found in ./ass2) autos: ▶ ✖ SEK
(gdb) break _main:38.003] [      ] [debug] Node: i ▶ ✖ SEK
Breakpoint 1 at 0x401000 [      ] [debug] Node: i ▶ ✖ SEK
(gdb) run 01 21:27:08.475] [      ] [debug] autos: ▶ ✖ SEK
Starting program: /home/kali/ass2 debug] autos: ▼ ✖ SEK
[2024-05-01 21:29:08.514] [      ] [debug] autos: ▶ ✖ SEK
Breakpoint 1, 0x0000000000401000 in _main() s: ▶ ✖ SEK
(gdb) i r 01 21:31:08.522] [      ] [debug] autos: ▶ ✖ SEK
rax 24-05-01 21 0x008.481] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rbx 24-05-01 21 0x008.471] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rcx 24-05-01 21 0x008.471] [      ] [d 0 0 g] autos: ▼ ✖ SEK
rdx 24-05-01 21 0x008.471] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rsi 24-05-01 21 0x008.474] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rdi 24-05-01 21 0x008.507] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rbp 24-05-01 21 0x008.486] [      ] [d 0 0 x 0] autos: ▶ ✖ SEK
rsp 24-05-01 21 0x7fffffffef310 [d 0 0 x 7fffffffef310]
r8 24-05-01 21 0x008.471] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r9 24-05-01 21 0x008.506] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r10 24-05-01 21 0x008.474] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r11 24-05-01 21 0x008.530] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r12 24-05-01 21 0x008.490] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r13 24-05-01 21 0x008.522] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r14 24-05-01 21 0x008.510] [      ] [d 0 0 g] autos: ▶ ✖ SEK
r15 24-05-01 21 0x008.478] [      ] [d 0 0 g] autos: ▶ ✖ SEK
rip 24-05-01 21 0x4010001] [      ] [d 0 0 x 401000 <_main>]
eflags 05-01 21 0x202.471] [      ] [d 0 [ IF ] autos: ▶ ✖ SEK
cs 24-05-01 21 0x333.471] [      ] [d 0 51] autos: ▶ ✖ SEK
ss 24-05-01 21 0x2b3.471] [      ] [d 0 43] autos: ▶ ✖ SEK
ds 24-05-01 21 0x008.470] [      ] [d 0 0 g] autos: ▶ ✖ SEK
es 24-05-01 21 0x008.471] [      ] [d 0 0 g] autos: ▶ ✖ SEK
fs 24-05-01 21 0x053.364] [      ] [d 0 0 g] Node: i ▶ ✖ SEK
gs 24-05-01 21 0x008.472] [      ] [d 0 0 g] autos: ▶ ✖ SEK (gdb)
```

```

(gdb) disas 21:25:08.509] [      ] [debug] autos:
Dump of assembler code for function _main:de:
=> 0x0000000000401000<+0>:      movabs $0x1,%rax
[200x000000000040100a<+10>:      movabs $0x1,%rdi
[200x0000000000401014<+20>:      movabs $0x402000,%rsi
[200x000000000040101e<+30>:      movabs $0xf,%rdx
[200x0000000000401028<+40>:      syscall autos:
[200x000000000040102a<+42>:      movabs $0x3c,%rax
[200x0000000000401034<+52>:      mov     $0x0,%edi
[200x0000000000401039<+57>:      syscall autos:
End of assembler dump.22] [      ] [debug] autos:
(gdb) set disassembly-flavor intel
(gdb) disas 21:33:08.471] [      ] [debug] autos:
Dump of assembler code for function _main:tos:
=> 0x0000000000401000<+0>:      movabs rax,0x1
[200x000000000040100a<+10>:      movabs rdi,0x1
[200x0000000000401014<+20>:      movabs rsi,0x402000
[200x000000000040101e<+30>:      movabs rdx,0xf
[200x0000000000401028<+40>:      syscall autos:
[200x000000000040102a<+42>:      movabs rax,0x3c
[200x0000000000401034<+52>:      mov     edi,0x0
[200x0000000000401039<+57>:      syscall autos:
End of assembler dump.30] [      ] [debug] autos:

```

```

(gdb) si-01 21:26:08.471] [ ] [debug] autos:
0x000000000040100a in __main () [debug] Node 1
(gdb) i r01 21:26:41.190] [ ] [debug] Node 1
rax 24-05-01 21:0x108.475] [ ] [0 1 g] autos:
rbx 24-05-01 21:0x008.527] [ ] [0 0 g] autos:
rcx 24-05-01 21:0x008.514] [ ] [0 0 g] autos:
rdx 24-05-01 21:0x008.488] [ ] [0 0 g] autos:
rsi 24-05-01 21:0x008.522] [ ] [0 0 g] autos:
rdi 24-05-01 21:0x008.481] [ ] [0 0 g] autos:
rbp 24-05-01 21:0x008.471] [ ] [0 0x0] autos:
rsp 24-05-01 21:0x7fffffffef310] [ ] [0 0x7fffffffef310]
r8 24-05-01 21:0x008.471] [ ] [0 0 g] autos:
r9 24-05-01 21:0x008.474] [ ] [0 0 g] autos:
r10 24-05-01 21:0x008.507] [ ] [0 0 g] autos:
r11 24-05-01 21:0x008.486] [ ] [0 0 g] autos:
r12 24-05-01 21:0x008.486] [ ] [0 0 g] autos:
r13 24-05-01 21:0x008.471] [ ] [0 0 g] autos:
r14 24-05-01 21:0x008.506] [ ] [0 0 g] autos:
r15 24-05-01 21:0x008.474] [ ] [0 0 g] autos:
rip 24-05-01 21:0x40100a0] [ ] [0 0x40100a0<_main+10]
eflags 05-01 21:0x202.490] [ ] [0 [ IF ] autos:
cs 24-05-01 21:0x338.522] [ ] [0 51] autos:
ss 24-05-01 21:0x2b8.510] [ ] [0 43] autos:
ds 24-05-01 21:0x008.478] [ ] [0 0 g] autos:
es 24-05-01 21:0x008.471] [ ] [0 0 g] autos:
fs 24-05-01 21:0x008.471] [ ] [0 0 g] autos:
gs 24-05-01 21:0x008.471] [ ] [0 0 g] autos:
(gdb) disas 21:51:08.471] [ ] [debug] autos:
Dump of assembler code for function __main:
[200x0000000000401000<+0>: movabs rax,0x1
=>00x000000000040100a<+10>: movabs rdi,0x1
[200x0000000000401014<+20>: movabs rsi,0x402000
[200x000000000040101e<+30>: movabs rdx,0xf
[200x0000000000401028<+40>: syscall autos:
[200x000000000040102a<+42>: movabs rax,0x3c
[200x0000000000401034<+52>: mov edi,0x0
[200x0000000000401039<+57>: syscall autos:
End of assembler dump.
(gdb) x/s 0x402000 08.486] [ ] [0 0 g] autos:
0x402000:01 21:5"Desec Security\n"

```

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

```

B+> 0x401000 <_main>      movabs $0x1,%rax
0x40100a <_main+10>      movabs $0x1,%rdi
0x401014 <_main+20>      movabs $0x402000,%rsi
0x40101e <_main+30>      movabs $0xf,%rdx
0x401028 <_main+40>      syscall
0x40102a <_main+42>      movabs $0x3c,%rax
0x401034 <_main+52>      mov $0x0,%edi
0x401039 <_main+57>      syscall
0x40103b                  add %al,(%rax)
0x40103d                  add %al,(%rax)
0x40103f                  add %al,(%rax)
0x401041                  add %al,(%rax)

```

native process 231236 In: _main

Reading symbols from ./ass2 ...

(No debugging symbols found in ./ass2)

(gdb) break _main

Breakpoint 1 at 0x401000

(gdb) run

Starting program: /home/kali/ass2

Breakpoint 1, 0x0000000000401000 in _main ()

(gdb) layout asm

(gdb) layout regs

(gdb) █

```
edb --run ass2
```

File View Debug Plugins Options Help

ass2: No Analysis Found

Address	Disassembly	Comment
00000000:00401000	48 b8 01 00 00 00 00 00	movabs rax, 1
00000000:0040100a	48 bf 01 00 00 00 00 00	movabs rdi, 1
00000000:00401014	48 be 00 20 40 00 00 00	movabs rsi, 0x402000
00000000:0040101e	48 ba 0f 00 00 00 00 00	movabs rdx, 0xf
00000000:00401028	0f 05	syscall
00000000:0040102a	48 b8 3c 00 00 00 00 00	movabs rax, 0x3c
00000000:00401034	bf 00 00 00 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
00000000:0040104d	00 00	add [rax], al

rax = 0x0000000000000000

Registers

Register	Value	Comment
RAX	0000000000000000	orig: 0000000000000000
RCX	0000000000000000	
RDX	0000000000000000	
RBX	0000000000000000	
RSP	00007ffd14470550	
RRP	0000000000000000	
RSI	0000000000000000	
RDI	0000000000000000	
R8	0000000000000000	
R9	0000000000000000	
R10	0000000000000000	
R11	0000000000000000	
R12	0000000000000000	
R13	0000000000000000	
R14	0000000000000000	
R15	0000000000000000	

RIP 0000000000401000 </home/kali/ass2>

C 0 ES 0000

Data Dump

0x0000000000401000-0x00000000

Address	Disassembly	Comment
00000000:00401000	48 b8 01 00 00 00 00 00	
00000000:00401010	00 00 00 00 48 be 00 20 40 0	
00000000:00401020	0f 00 00 00 00 00 00 0f 0	
00000000:00401030	00 00 00 00 bf 00 00 00 00 0	
00000000:00401040	00 00 00 00 00 00 00 00 00 0	
00000000:00401050	00 00 00 00 00 00 00 00 00 0	
00000000:00401060	00 00 00 00 00 00 00 00 00 0	
00000000:00401070	00 00 00 00 00 00 00 00 00 0	
00000000:00401080	00 00 00 00 00 00 00 00 00 0	
00000000:00401090	00 00 00 00 00 00 00 00 00 0	
00000000:004010a0	00 00 00 00 00 00 00 00 00 0	
00000000:004010b0	00 00 00 00 00 00 00 00 00 0	
00000000:004010c0	00 00 00 00 00 00 00 00 00 0	

Stack

Address	Disassembly	Comment
00007ffd:14470550	0000000000000001	ASCII "ass2"
00007ffd:14470558	00007ffd14472609	ASCII "COLORTERM=truecolor"
00007ffd:14470560	00007ffd14472622	ASCII "DISPLAY=:0"
00007ffd:14470568	00007ffd1447262d	ASCII "LANG=C.UTF-8"
00007ffd:14470570	00007ffd1447263a	ASCII "LANGUAGE="
00007ffd:14470578	00007ffd14472644	ASCII "PATH=/usr/local/sbin:/usr/local/bin:/l
00007ffd:14470580	00007ffd144726a2	ASCII "TERM=xterm-256color"
00007ffd:14470588	00007ffd144726b6	ASCII "XAUTHORITY=/home/kali/.Xauthority"
00007ffd:14470590	00007ffd144726d8	ASCII "XDG_CURRENT_DESKTOP=XFCE"
00007ffd:14470598	00007ffd144726f1	ASCII "LS_COLORS=rs=0:di=01;34:ln=01;36:mh=0
00007ffd:144705a0	00007ffd14472e14	ASCII "MAIL=/var/mail/root"
00007ffd:144705a8	00007ffd14472e28	ASCII "LOGNAME=root"
00007ffd:144705b0	00007ffd14472e35	ASCII "USER=root"

Stack Debugger Error Console

paused