GDB: Extra

Marcus Botacin

Minicurso

2018

Roteiro

1 Identificação Manual do Entry Point.

Roteiro

1 Identificação Manual do Entry Point.

Etapas

- Encontrar o *entry point* do binário.
- Definir um *breakpoint* neste ponto.
- Executar até ser interrompido.
- Identificar o endereço da *main* na `libc`.
- Definir um *breakpoint* neste ponto.
- Executar até a *main*.

Entry Point do binário.

```
(gdb) file /bin/ls
Lendo símbolos de /bin/ls...(no debugging symbols
(gdb) info files
Symbols from "/bin/ls".
Local exec file:
        `/bin/ls', tipo de arquivo elf64-x86-64
        Entry point: 0x4049a0
```

Figure: Identificando o *Entry Point*.

Entry Point do binário.

```
Breakpoint 1, 0x00000000004049a0 in ?? ()
(gdb) x/13i $rip
=> 0x4049a0:    xor    %ebp,%ebp
   0x4049a2:    mov    %rdx,%r9
   0x4049a5:    pop    %rsi
   0x4049a6:    mov    %rsp,%rdx
   0x4049a9:    and    $0xfffffffffffffff0,%rsp
   0x4049ad:    push   %rax
   0x4049ae:    push   %rsp
   0x4049af:    mov    $0x413c20,%r8
   0x4049b6:    mov    $0x413bb0,%rcx
   0x4049bd:    mov    $0x402a00,%rdi
```

Figure: Identificando a função *main*.