GSOC'18 - Cutter Debugging and Emulation support

r2con // September 8th 2018 mandlebro Filipe Casal

Cutter



- radare2's GUI
- Supports most essential r2 features
- FOSS
- Developed in Qt C++
- https://github.com/radareorg/cutter

Google Summer of Code project

Implement Debugging and Emulation support in Cutter

Major goals:

- Independent seeks & Multiple widgets
- Debug & Emulation support

Independent seeks

You can now have different widgets with different seeks.

```
\leftarrow
                                                                                                             Disassembly Graph (entry0) Hexdump Strings Search
     sub.__gmon_start_5b0
   sym. do global dtors aux
                                                                                                                                                                                                                                                           xor ebp, ebp; [14] -r-x section size 754 named .tex
mov r9, rdx
pop rpi
mov rdx, rsp
     sym.deregister_tm_clones
                                                                                                                                                                                                                                                     push rad
push ra
                                                                                                                                                                                                                                                                mov eax, 0x601067
      ym.register_tm_clones
                                                                                                                                                                                                                                                              push rbp
sub rax, obj.completed.7596
                                                                                                                                                                                                                                                                cmp rax, 0xe
                                                                                                                                                                                                                                                                mov rbp, rsp
                                                                                                                                                                                                                                                                pop rbp
mov edi, obj.completed.7596 ; obj.__TMC_END ; 0x601068
        > Populating UI
             - ((fn [f s n] (cat [(f f s n) "dare2"])) (fn [f s n] (pr s) (lf (> n 0) (f f (cat [s "ra"]) (dec n)) s)) ** Infty)
```

Multiple panels

You can now open more than one instance of the same widget

```
The Edit Vew Windows Debug Help

Type flag same or editors here

Cash (main) foot years)

Touction

Toucti
```

Debugging, Emulation & Attaching

Menus:

- Debug toolbar
- Context menu

Widgets:

- Registers
- Stack
- Breakpoints
- Backtrace
- Register references
- Memory maps

Debugging, Emulation & Attaching

Major Issues:

- Ptrace & multiple threads
- Handling stdin

ESIL

- Evaluable Strings Intermediate Language
- General intermediate representation
- Allows to emulate most architectures r2 supports!

Implemented features:

- Breakpoints now work in ESIL emulation
- ESIL continue until call: aecc
- Eval variable to break emulation on invalid instructions:
 - e esil.breakoninvalid

Thank you! Thanks to xarkes, Florian and Maijin for the support during the project!

Questions?



```
@filipe_casal
```