radare2 Reverse engineering toolkit

CONCEPTS

Commands are short letter chains: append ? to any prefix (a?, p?, pd?) to list what it offers.

Open r2 file
↓ `aaa`
Analyse functions, xrefs
↓ `s / pdf`
Inspect seek + print
↓ `w / ood`
Patch or debug write, step

Almost everything acts at the current seek; use cmd @ addr to run it elsewhere without moving.

OPEN AND ANALYSE

`r2 -A <file>`
Open and run full analysis

`r2 -d <file>`
Open under the debugger

`r2 -q -c '<cmds>' <file>`
Run commands and quit

`aaa`
Deeper analysis of calls and refs

`afl`
List functions

`axt <addr>`
Find references to an address

BINARY INFO

`iI`
Binary info and protections

`iz`
Strings in data sections

`ii`
Imported functions

SEEK AND PRINT

`s <addr>`
Seek to address, flag or function

`pdf`
Disassemble current function

`pd <n>`
Disassemble n instructions

SEEK AND PRINT (cont.)

`px [len]`
Hexdump

`<cmd> @ <addr>`
Run cmd at addr without seeking

`<cmd>~<text>`
Grep the output

VISUAL MODE

`V`
Enter visual mode

`VV`
Graph view of function

`p / P`
Cycle print modes

`Enter`
Follow jump or call

`x / X`
Xrefs to / from here

`:`
Run a command

`q`
Back to shell

SEARCH

`/ <text>`
Search for a string

`/x <hex>`
Search hex bytes

WRITE AND PATCH

`wx <hex>`
Write hex bytes

DEBUGGER

`ood [args]`
Reopen file in debug mode

`dc`
Start or continue

`db <addr>`
Set breakpoint

`ds [n]`
Step into

`dr`
Show registers