Actually using radare2

Vasilij Schneidermann

June 2019

Outline

Section 1

Actually using radare2

About

- Vasilij Schneidermann, 26
- Software developer, bevuta IT GmbH
- mail@vasilij.de
- `https://github.com/wasamasa`
- radare2 contributor
- I use it for all things binary

What's radare2?

- Initially: Forensics toolkit (raw data recovery)
- Hex/memory editor
- RE toolkit (assembler/disassembler/analysis)
- Binary exploitation toolkit (ROP/shellcode)
- Debugger
- Anything thanks to scripting

Why would I want to use it?

- It feels like Vim and Emacs combined
- Textual UI
- Portable, self-contained
- Flexible, scriptable
- Easy to contribute to

Why would I want to not use it?

- It feels like Vim and Emacs combined
- Buggy, high churn
- Docs could be better
- Not up to par to commercial tools (decompilation particularly)

How do I start using it?

- Launch `r2 crackme`
- Do some analysis (`aaa`)
- Enter visual mode (`v`)
- Change to disassembly view (`p`)
- Go to main function (`g main`)
- Jump between sections (`n`/`N`)
- Read decompiled code (`:pdc`, requires `r2pm -i r2dec`)
- View call graph (`V`)

How do I figure out things?

- Append `?` to a command to get help
- Press `?` in visual (panel) mode
- https://radare.gitbooks.io/radare2book/content/
- `#radare` channel on Freenode
- Bridges to Telegram group

Commands worth remembering

- `p` (print)
- `w` (write)
- `s` (seek)
- `?` (help)
- Look up the rest

Still stuck?

Demo time

- Steganography
- CHIP-8 analysis
- Crackme 1 & 2