Wa-r2-Con

2016 edition

pancake <pancake@nopcode.org>

Who Am I?

pancake, aka the author of r2 and many other stuff
  (sdb, acr, valabind, mesure, wistumbler2, ...)

https://twitter.com/radareorg
https://twitter.com/trufae
https://github.com/radare
https://github.com/trufae
https://bitbucket.org/trufae
https://lolcathost.org
http://youterm.com
http://nopcode.org
https://rada.re
...

Some background

- Optimizing MM codecs for mips and arm
- RE Sexy Panda at the Defcon CTF
- Research Bluetooth security
- Into the VX DOS scene
- Restless developer
- Forensic Analyst
- NetBSD packager
- Cmdline cowboy
- Bitcoin trader
- iOS researcher
- Python hater
- ...
- Got a CVE for XNU \o/

Preconditions

- Who knows what radare is?
- Who uses r2 here?
- When was last time you compile it?

TOO OLD

People use

- Metasploit / Canvas / RopGadget
- BinWalk / File / Strings
- EnCase / Photorec
- gdb / windbg / olly
- IDA / Hopper
- HexRays decompiler
- Python
- Unicorn / QEMU
- Apt−Get
- Nasm / Gas / Gcc
- www.telepizza.com

But I do

- r2

Why that?

- An OpenSauce hexadecimal editor
- Everything from scratch in C, no deps
- Multiarch / Multiformats
- Always growing community
- Reverse Engineering Framework
- Portability / Embedding
- Optimized for the shell
- Scripting with any language
- Dependencies, packages, scripts r2pm
- Fast fixing opensource (actively fuzzed and fixes in <24h)
- Embedded webserver
- Collecting small tools
- ...

What Can It Do?

- Forensics
  - partitions, mount fs, carve dumps, magic, blockhashing
- Exploiting
  - analyze crashes, emulate rop, stack analysis, ..
- Shellcoding
  - generate shellcodes, payloads, ...
- Cracking
  - binary patching, low level debugger
- Bindiffing
  - byte level, delta diffing, code diffing
- Reverse Engineering
  - decompilation, xrefs, graphs, strings

But some hackers ... (sad but true facts)

- Are scared of using the terminal
- Don’t want to spend time learning new tools
- Doesn’t know how to compile C projects
- Afraid of reading code instead of documentation
- Only use Python stuff

User Interface

- Several web interfaces
- Bokken (Py–GTK)
- Blessr2
- Some Unreleased GTK and QT GUIs)
- .NET

DEMO

Decompile

- Better understanding of code, structures, ...

- Disassemble
- Graphs in Ascii art / GraphViz / Web
- Pseudo Disassembly
- Pseudo Decompilation
- Decompilation (Radeco)
- Problem Solving (Rune)

DEMO

ESIL

- Forth like VM with 2 stacks and 109 instructions
- Each instruction is translated into a oneliner expression
- No FPU or MMX support yet
- Supports 15 different CPUs (rasm2 -L | grep Ae)
- Translates to REIL

ESIL

Useful for:

- emulation of many archs in a generic way
- searching with complex conditionals
- analyzing side effects
- bindiffing at micro−instruction level
- transpilation between architectures
- decompilation to higher level representations
- advanced rop gadget searching

DEMO

r2pipe

– Easiest way to script r2 from real programming languages
– Supoprts 17 langs (C, Go, Python, Swift, Rust, C#, Vala, Java, Ruby,..)
– Simplest bindings, but there are also real API bindings

DEMO

Debugging

- Native support for Linux/OSX/Windows/iOS/Android
- Remoting with GDB, WinDBG, Bochs, QNX (qemu, ..
- In process injection
- Low level debugger
- Injecting payloads

Exploiting

- Register / Memory telescoping
- Code Injection
- Backtraces
- Tracing
- Upcomming heap analysis support
- ...

RAROP2 DEMO

R2CON

After 10 years of development...

Location: Barcelona
Dates: September 8, 9, 10

http://rada.re/con

Thanks to...

- Nighterman – for some demos
- RevSkills – for the fuzzing
- dan1t0 – for the tshirts
- warcon – for having me

Questions?