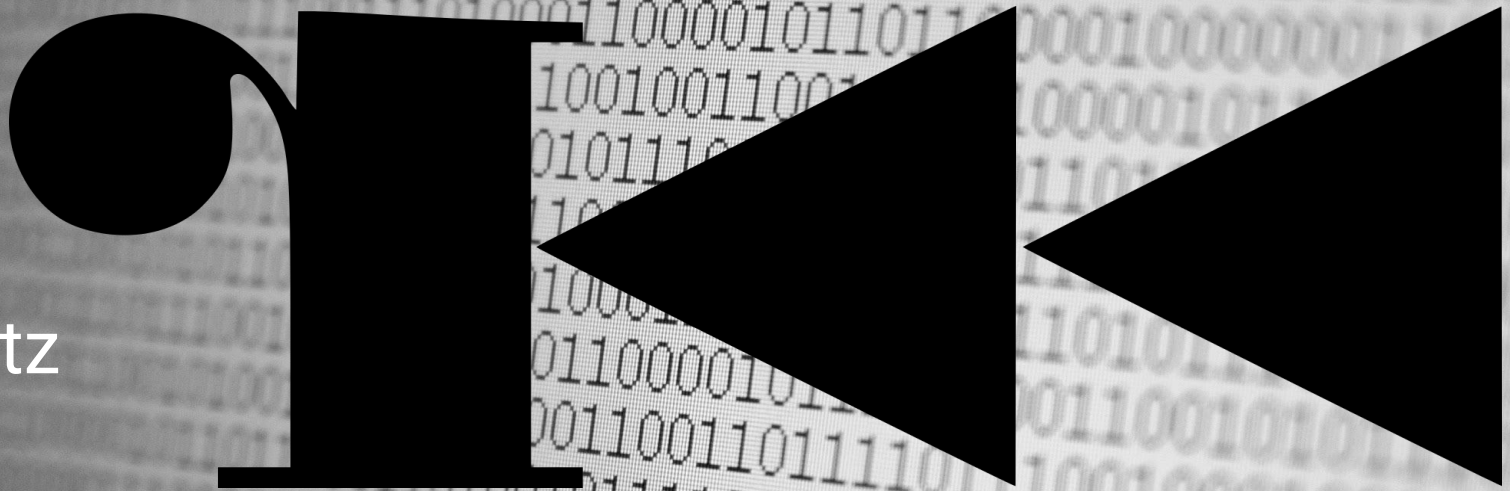
r2

Noah Kritz



whoami

> ~~root~~ noah

School

Senior @ *OSU* | Graduating May ‘19
Computer Science & Engineering

Work

Co-op @ *Battelle* | August ‘17 - *present*
Recently accepted full-time offer

Interests

Reverse engineering & vulnerability analysis
Web stuff - Node.js & React in particular

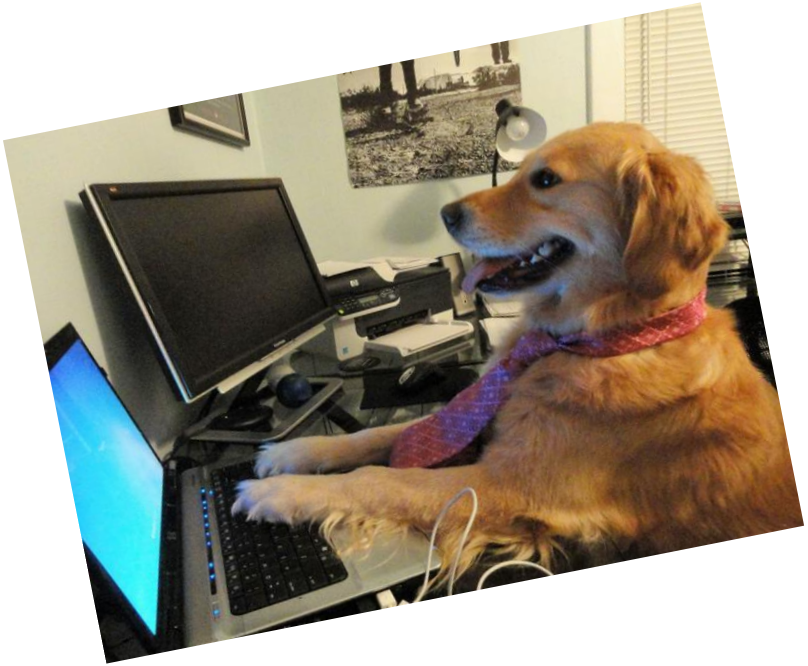
TODO

- ➔ What *exactly* is Radare2?
- ➔ Brief Tools Overview
- ➔ Brief Commands Overview
- ➔ Decompiler?
- ➔ Installing & Updating
- ➔ Play time
- ➔ Questions

What *exactly* is Radare2 … ?

- ➔ A *free* & *open source* reverse engineering ***framework***
  - ◆ Set of command-line tools that can be used together or independently
- ➔ RA-DA-RE stands for RAw DAta REtrieval
  - ◆ Originally built as a forensics tool
- ➔ Disassemble / assemble for many different architectures
- ➔ Compatible with Linux, *BSD, Windows, OSX, Android, iOS, Solaris, etc.
- ➔ Debug with native and remote debuggers (gdb, webui, r2pipe, windbg, etc.)
- ➔ Can be scripted w/ Python, Node, and more. [r2pipe]
- ➔ *Notorious for a high learning curve*
- ➔ r2 will be the vi of reverse engineering in years to come

R2 LEARNING CURVE



DIFFICULTY

GIT CLONE

R2 /BIN/LS ANYTHING USEFUL

Brief

Tools

Overview

- Radare2
  - The main tool. Uses the core hexadecimal editor and debugger. Can be scripted with r2pipe.
- Rabin2
  - Extracts information from binaries. Used by the core to get symbols, file info, x-references, etc.
- Rasm2
  - Command line assembler / disassembler
- Rahash2
  - Baked in block-based hash tool
- Radiff2
  - Binary diffing with multiple algorithms
- Rafind2
  - Finds byte patterns in files
- Ragg2
  - Compiles programs into tiny binaries. Front-end for r_egg
- Rarun2
  - Launcher that can programs in different environments, with different arguments, different permissions, different directories, etc.
- Rax2
  - Minimalistic mathematical expression evaluator

Brief

Commands

Overview

- ➔ Documented in C
  - ◆ ?
    - alone prints all possible commands, appended to a command prints detailed help about that command
- ➔ Commands that do *mostly* everything
  - ◆ pd
    - print disassembly
  - ◆ aa
    - analyze all functions & symbols
  - ◆ afl
    - list all functions
  - ◆ s
    - seek
  - ◆ w
    - write
  -  ◆ V
    - visual mode
  - ◆ q
    - quits

Brief

Commands

Overview

continued...

- ➔ ***Inside*** visual mode
  - ◆ ?
    - prints visual mode help
  - ◆ p
    - toggles print modes (hex, disasm, debug, words, buf)
  - ◆ V
    - graph mode
  - ◆ !
    - window mode
  - ◆ c
    - cursor mode

Brief

Commands

Overview

continued...

continued...

- Each character in the command is a sub command of the previous one
  - p?
    - prints usage of ‘p’
  - px
    - print hexdump
  - pxw
    - print hexdump of words
  - pxw 12
    - Print 12 bytes of a hexdump of words

Brief

Commands

Overview

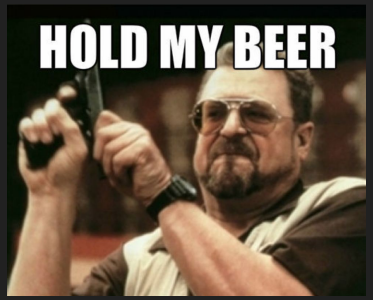
continued...

continued...

continued...

- Helpful commands I always find myself using
  - axt
    - references *to* current address
  - axff
    - references from current function
  - fs
    - manage flag spaces (f prints flags)
  - ~
    - Radare's internal grep tool
  - /
    - built-in search tool
  - pdj~{}
    - print disassembly prettified json
  - ? 42 * 12
    - evaluate math expression

But… Decompiler … & Hex-Rays?



- ➔ R2pm
  - ◆ Package manager for radare
- ➔ R2dec
  - ◆ Radare2's decompiler

Install

```
> r2pm init
> r2pm -i r2dec
… done.
```

Using

```
> r2 -A /bin/ls
> pdd
...
```

```
/* r2dec pseudo C output */
#include <stdint.h>

void entry0 (int32_t arg3) {
    ebp = 0;
    r9 = rdx;
    rdx = rsp;
    r8 = 0x00016c10;
    rcx = 0x00016ba0;
    rdi = main;
    __libc_start_main ();
    return _hlt ();
}
[0x00006130]>
```

But… ~~Decompiler~~ … ~~Hex-Rays~~? ... r2dec ✓

Renaming variables

> ...
> afvn foo arg3
> pdd
> ...

```
/* r2dec pseudo C output */
#include <stdint.h>

void entry0 (int32_t foo) {
    ebp = 0;
    r9 = rdx;
    rdx = rsp;
    r8 = 0x00016c10;
    rcx = 0x00016ba0;
    rdi = main;
    __libc_start_main ();
    return _hlt ();
}
```

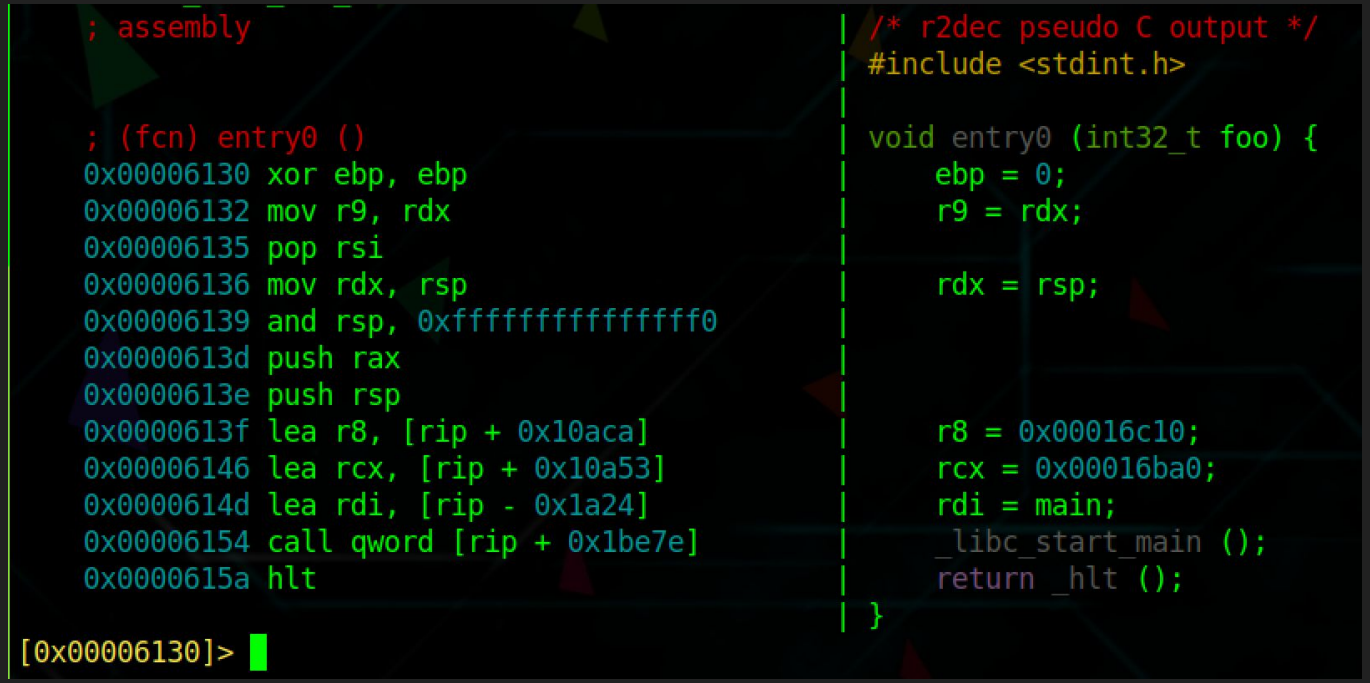
But… ~~Decompiler~~ … ~~Hex-Rays~~? ... r2dec ✓

Comparing w/ assembly

> …

> pdda

> …



Installing & Updating Radare

Install

git clone git@github.com:radare/radare2.git
cd radare2 && sys/install.sh

Update

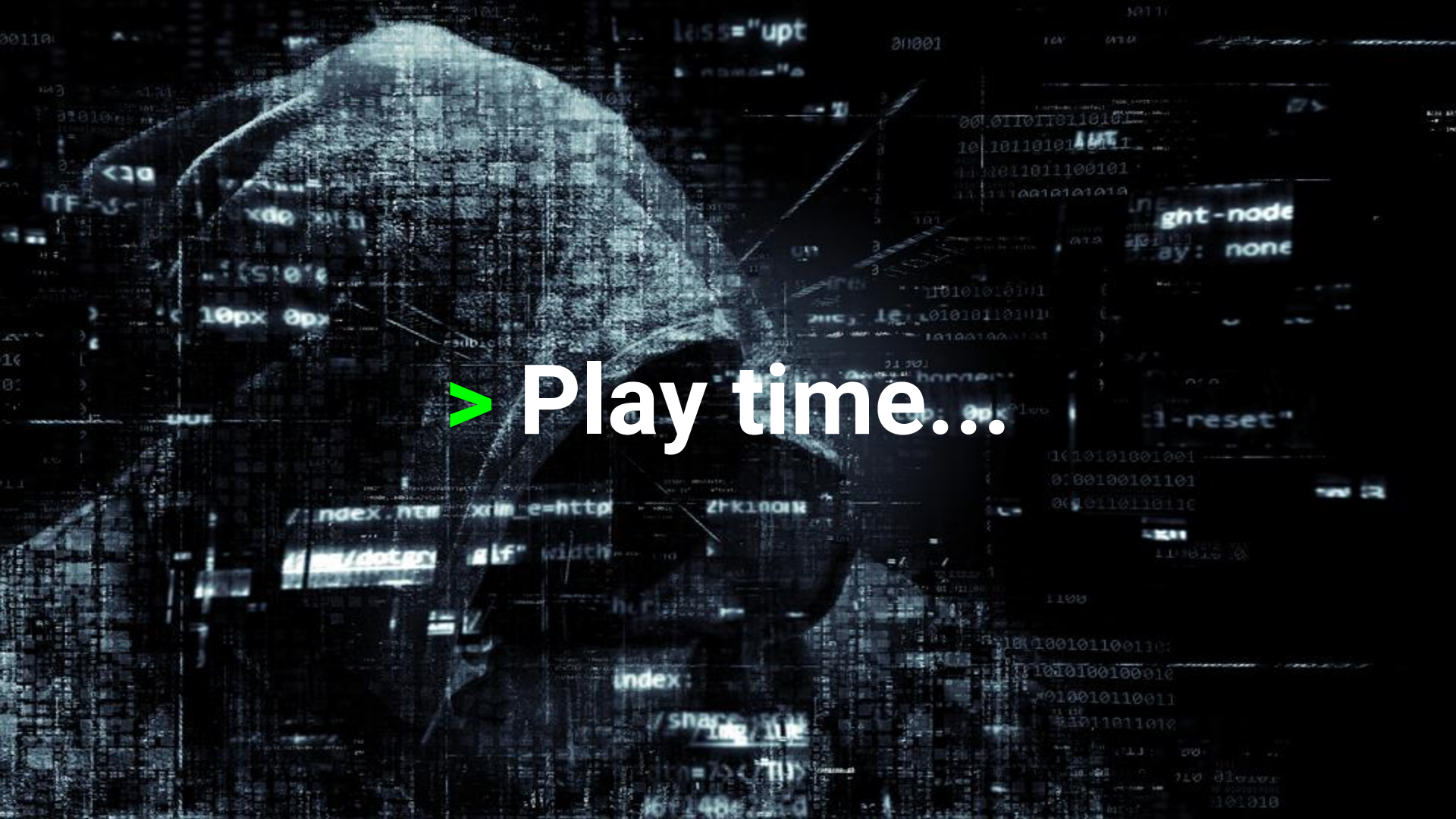
cd radare2 && sys/install.sh

r2Playground

Install

git clone git@github.com:kr1tzb1tz/r2Playground.git

➔ Going over the *r2Playground/Intro* module


> Play time...

Next time … ?

- ➔ Scripting r2 w/ r2pipe
- ➔ Project management
- ➔ More in depth debugging
- ➔ Customizing
- ➔ and more…

Questions?

Contact

➔ https://github.com/kr1tzb1tz

➔ https://twitter.com/kr1tzb1tz