Flipping malware with flip.re

Designing an interactive malware analysis system

Lars Haukli
@zutle
lars@flip.re

The flip.re project

Startup based in Oslo and Warsaw

Team of former sandbox developers from the anti-malware industry

“Empower your security team to
reverse engineer malware blazingly fast”

Analyzing malware fast

Combining the powers of dynamic and static analysis techniques

Dynamic (behavior) analysis is fast, but inaccurate

Static (code) analysis is detailed, but slow

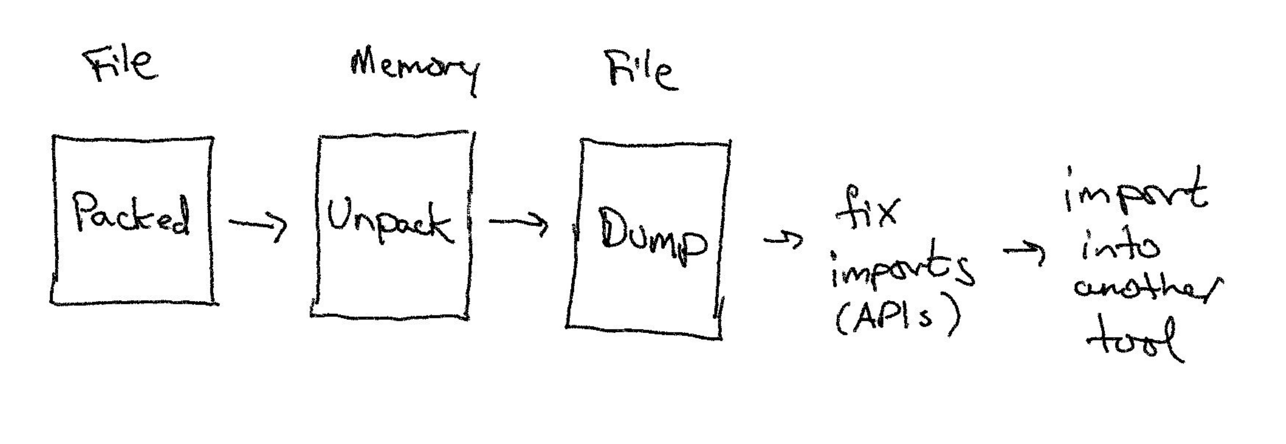
Targeted threats and evasive malware

Expect them to not run in a sandbox

Expect them to be undetected for a long time

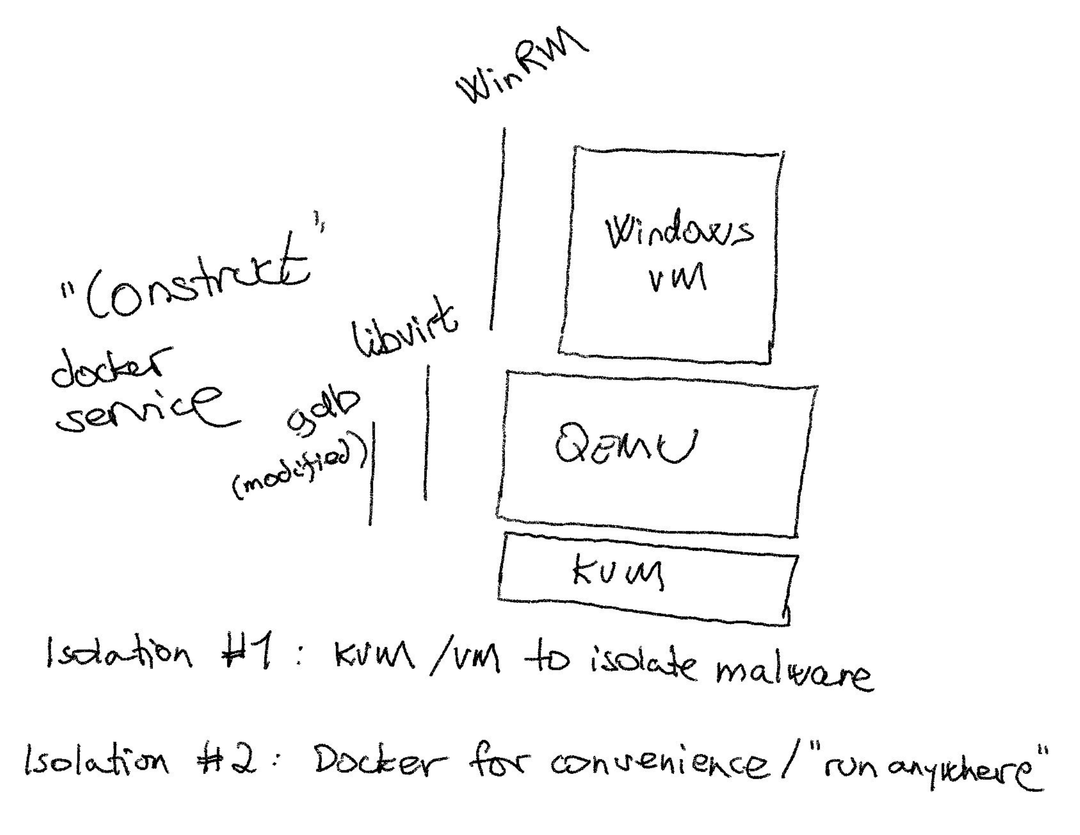
Actively makes malware analysis challenging

Debug, dump, import, repeat



The design

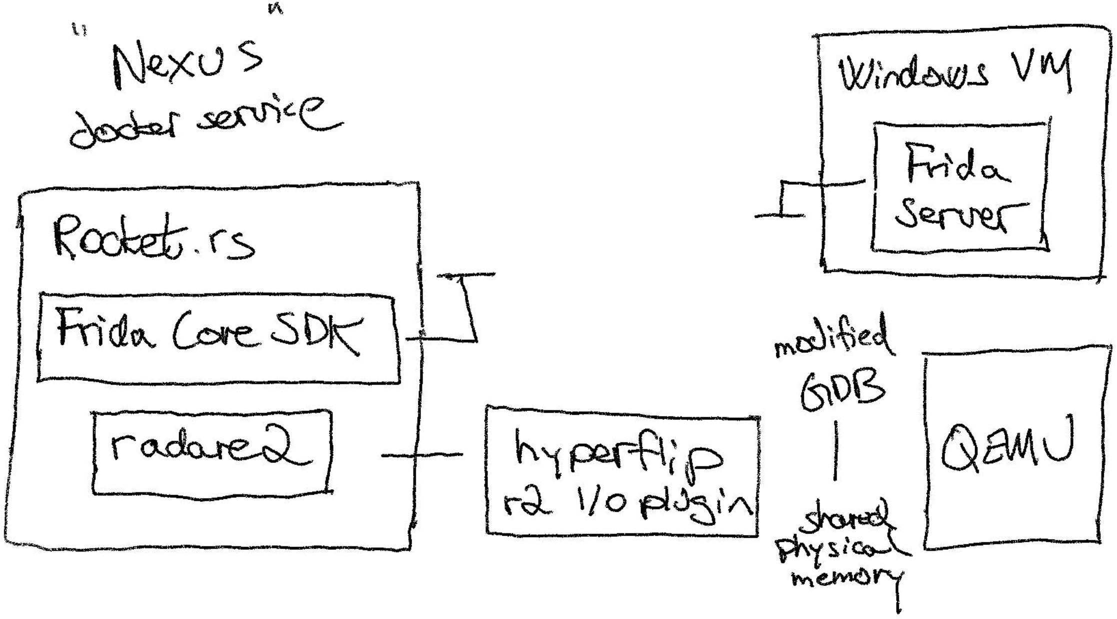
Isolation



Isolation #1 : KVM / VM to isolate malware

Isolation #2 : Docker for convenience / "run anywhere"

Monitoring



Version 1 uses Frida for event generation

In version 2 we plan to add VMI (hypervisor-level events)

Frida

Load programs inside the Windows VM (via Frida server)

Hook any user-mode function we ask it to, and report whenever they are called

Extremely flexible can be tailored to
individual samples/families

Hyperflip: I/O plugin for r2

Turns r2 into a hypervisor-level debugger

- Debug code running inside a Windows VM from the outside
- Full access to the entire virtual address space (all processes + kernel)
- Super powers (even hidden from the OS)

See my talk at r2con 2020

Hyperflip upgrades

Now supports multiple CPUs and “infinite” RAM

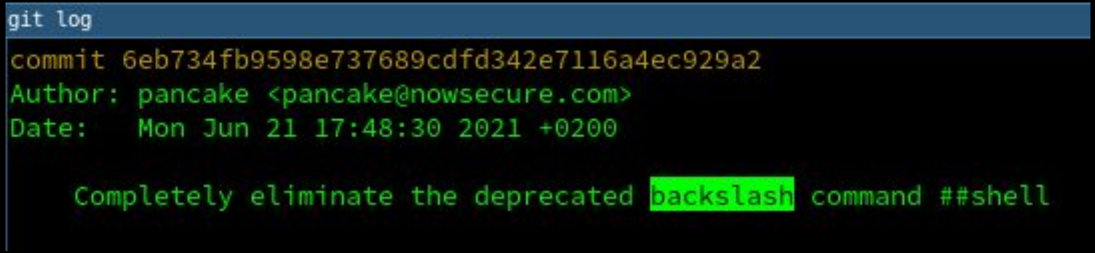
- Big thanks to defragger for lots of testing on his special “QA” system to trigger all the edge case bugs :)

Multi-CPU complicates everything,
but we decided it would be hard to add later,
and it will be important for UX

Special hyperflip r2 commands

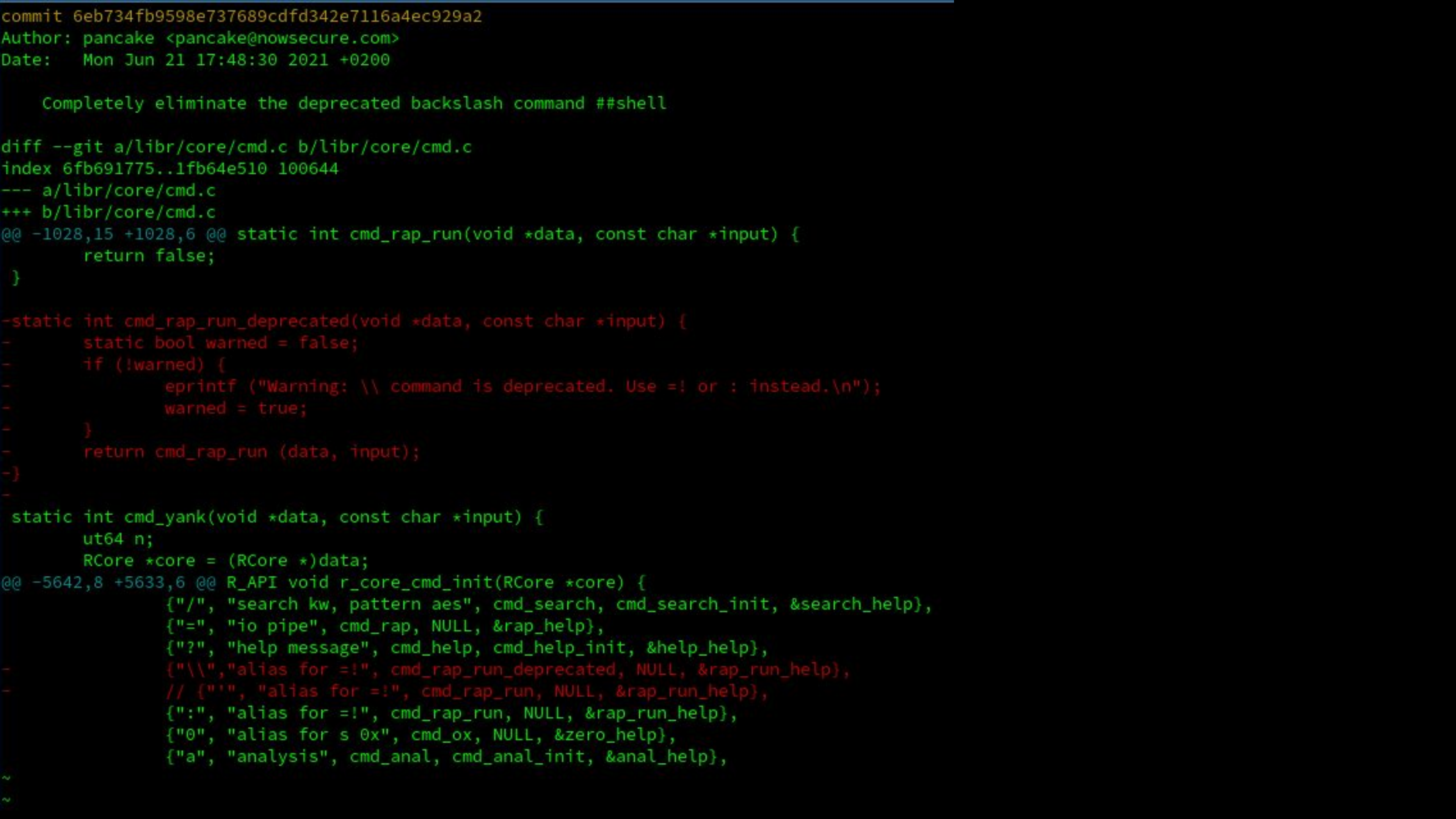
- I/O plugins can implement their own commands in r2

- The command to detach for a VM used to be \d



```
commit 6eb734fb9598e737689cdfd342e7116a4ec929a2
Author: pancake <pancake@nowsecure.com>
Date:   Mon Jun 21 17:48:30 2021 +0200

    Completely eliminate the deprecated backslash command ##shell
```



```
commit 6eb734fb9598e737689cdfd342e7116a4ec929a2
Author: pancake <pancake@nowsecure.com>
Date:   Mon Jun 21 17:48:30 2021 +0200

    Completely eliminate the deprecated backslash command ##shell

diff --git a/libr/core/cmd.c b/libr/core/cmd.c
index 6fb691775..1fb64e510 100644
--- a/libr/core/cmd.c
+++ b/libr/core/cmd.c
@@ -1028,15 +1028,6 @@ static int cmd_rap_run(void *data, const char *input) {
        return false;
 }

-static int cmd_rap_run_deprecated(void *data, const char *input) {
-       static bool warned = false;
-       if (!warned) {
-               eprintf ("Warning: \\ command is deprecated. Use =! or : instead.\n");
-               warned = true;
-       }
-       return cmd_rap_run (data, input);
-}
-
 static int cmd_yank(void *data, const char *input) {
        ut64 n;
        RCore *core = (RCore *)data;
@@ -5642,8 +5633,6 @@ R_API void r_core_cmd_init(RCore *core) {
                {"/", "search kw, pattern aes", cmd_search, cmd_search_init, &search_help},
                {"=", "io pipe", cmd_rap, NULL, &rap_help},
                {"?", "help message", cmd_help, cmd_help_init, &help_help},
-               {"\\","alias for =!", cmd_rap_run_deprecated, NULL, &rap_run_help},
-               // {"'", "alias for =!", cmd_rap_run, NULL, &rap_run_help},
                {":", "alias for =!", cmd_rap_run, NULL, &rap_run_help},
                {"0", "alias for s 0x", cmd_ox, NULL, &zero_help},
                {"a", "analysis", cmd_anal, cmd_anal_init, &anal_help},
~
~
```

Some hyperflip commands

:a - analyze memory (currently only to get PE entrypoint)

:drx, :drxe - hardware breakpoint (on entrypoint)

:cpu - display or modify CPU target

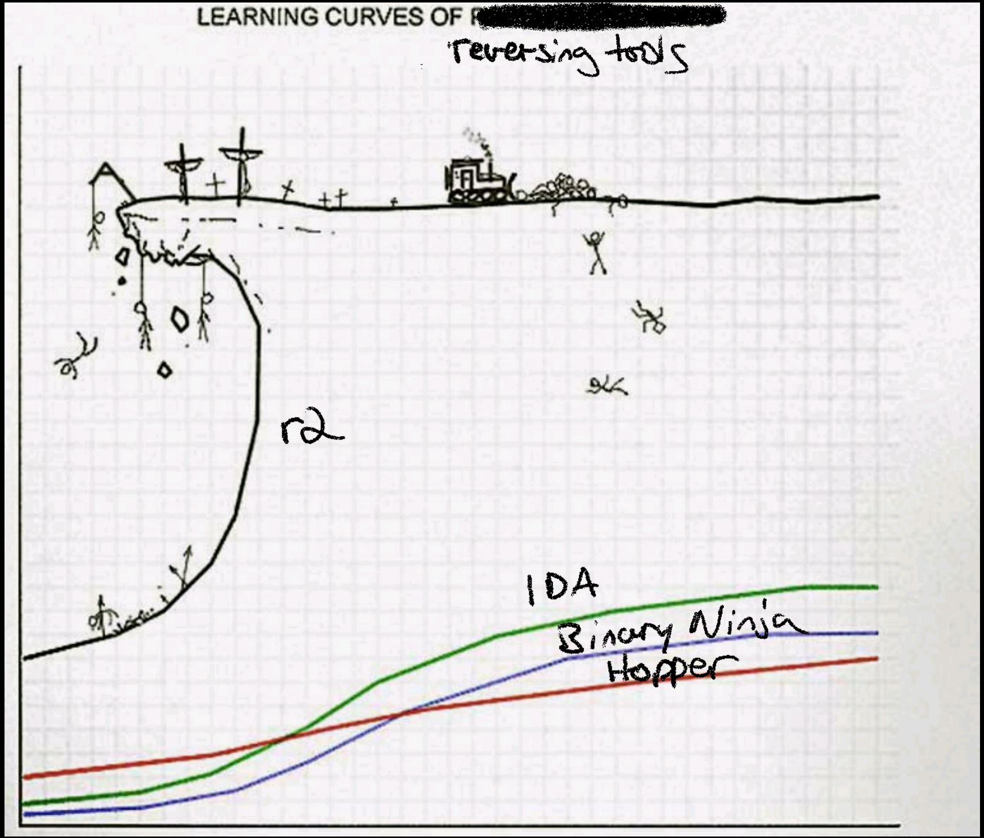
:k, :u - kernel mode, user mode

:l, :t - display live process, target process

:D - detach from VM

Combine these things… and...

UI/UX


LEARNING CURVES OF [redacted]
reversing tools
r2
IDA
Binary Ninja
Hopper

UI/UX

Web technology has become really nice and shiny

Look at e.g. Visual Studio (electron)

Our system should be able to run anywhere,
including the cloud, so accessing it
from a browser makes a lot of sense

UI: Frontflip

Based on the Next.js framework (thanks Jerry for helping out!)

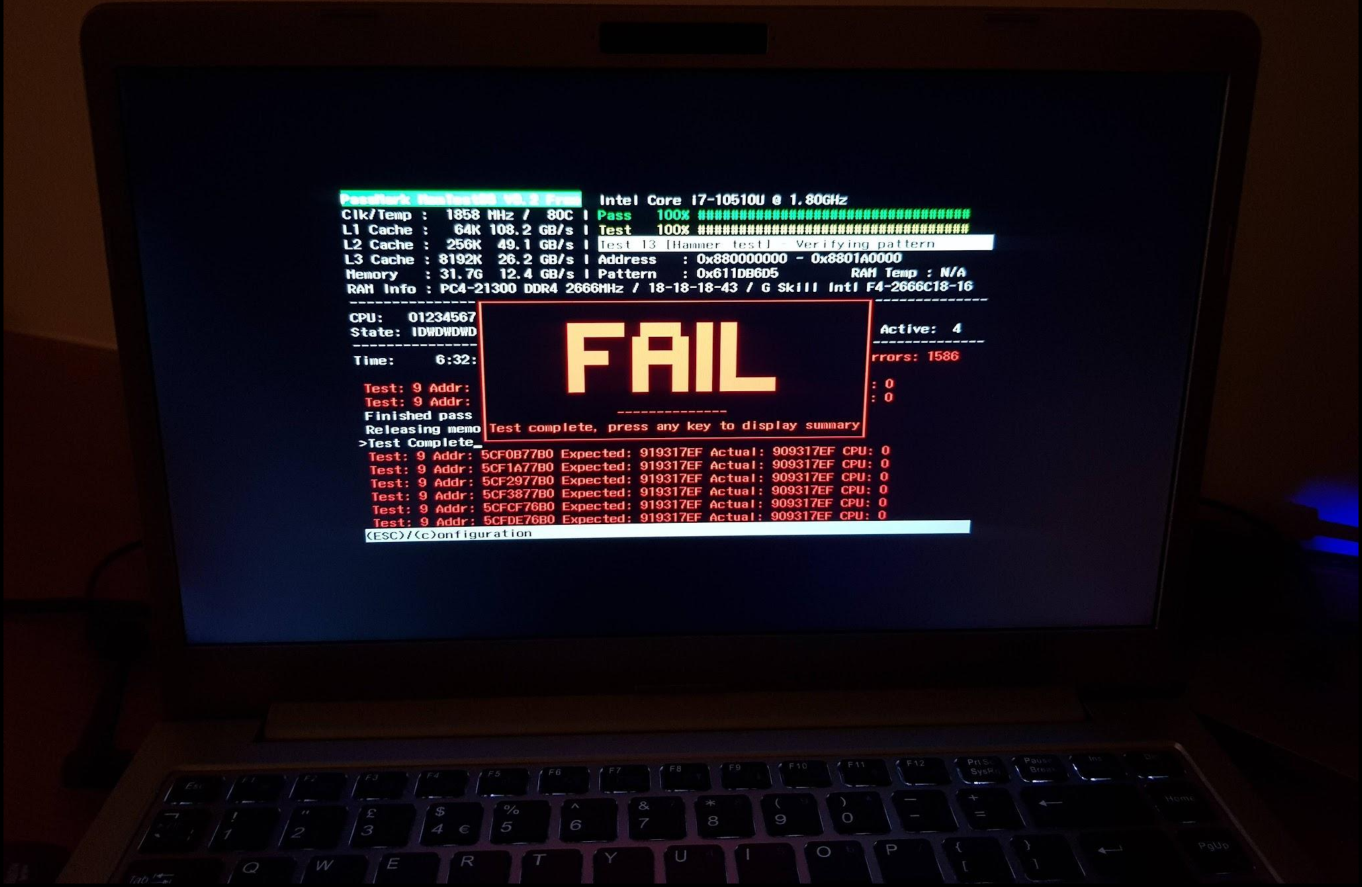
Uses the noVNC javascript library to connect with QEMU’s websocket VNC

Uses Xterm.js to bring r2 terminals to the browser via node-pty

- Maintained by Microsoft,
  and used in e.g. Visual Studio

Frida events streamed to the UI with socket.io

Live demo time :)



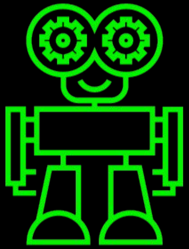
```
PassMark MemTest86 V9.2 Free  Intel Core i7-10510U @ 1.80GHz
Clk/Temp :  1858 MHz /  80C | Pass    100% ##########################################
L1 Cache :   64K 108.2 GB/s | Test    100% ##########################################
L2 Cache :  256K  49.1 GB/s | Test 13 [Hammer test] - Verifying pattern
L3 Cache : 8192K  26.2 GB/s | Address   : 0x880000000 - 0x8801A0000
Memory   : 31.7G  12.4 GB/s | Pattern   : 0x611DB6D5           RAM Temp : N/A
RAM Info : PC4-21300 DDR4 2666MHz / 18-18-18-43 / G Skill Intl F4-2666C18-16
---------------                                                 ---------------
CPU:   01234567                                                 Active:  4
State: IDWDWDWD              FAIL                               ---------------
---------------                                                 rrors: 1586
Time:     6:32:

  Test: 9 Addr:                                                 : 0
  Test: 9 Addr:                                                 : 0
  Finished pass                  --------------
  Releasing memo Test complete, press any key to display summary
 >Test Complete_
  Test: 9 Addr: 5CF0B77B0 Expected: 919317EF Actual: 909317EF CPU: 0
  Test: 9 Addr: 5CF1A77B0 Expected: 919317EF Actual: 909317EF CPU: 0
  Test: 9 Addr: 5CF2977B0 Expected: 919317EF Actual: 909317EF CPU: 0
  Test: 9 Addr: 5CF3877B0 Expected: 919317EF Actual: 909317EF CPU: 0
  Test: 9 Addr: 5CFCF76B0 Expected: 919317EF Actual: 909317EF CPU: 0
  Test: 9 Addr: 5CFDE76B0 Expected: 919317EF Actual: 909317EF CPU: 0
(ESC)/(c)onfiguration
```

Join us!

We are looking for

- Security teams interested in early access
- Smart people to join our team



Lars Haukli
@zutle
lars@flip.re

Thank you :)

Lars Haukli
@zutle
lars@flip.re