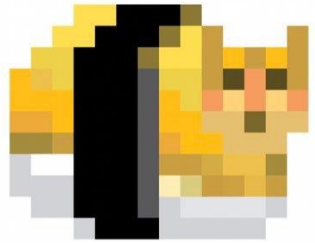
Depurant una Gameboy amb R2Frida

De la mà de pancake

Introducció



Qui sóc

- Pancake (aka Sergi Àlvarez)
- Autor de r2 i r2frida.. I un grapat de projectes opensource més
- Mobile Sec Analyst a NowSecure

De què parlem

- Jugant amb Frida, R2 i la GB
- He triat l'emulador SDL GNU Boy
- Introducció a r2frida per emuladors

Radare2?

- 100% **software lliure**
- Projecte personal que ha crescut a colaboratiu i q vaig començar fa 15 anys
- Sistema operatiu que pot fer-se servir com a editor hexadecimal
- Escrit en C, centrat amb la portabilitat, filosofia UNIX
- Molt extensible i configurable i facil d'automatitzar amb r2pipe
- Permet desensamblar, emular i decompilar bastantes arquitectures diferents
- Corva d'aprenentatge acceptable

Hora de la demo!

- Revisem el codi del plugin i com funcionen els plugins de r2frida
- Com interceptar les crides a lectura i escriptura de memòria
- Noves comandes disponibles comparteixen dades de l'agent al host.

APM?

Per més informació sobre el projecte entreu a GitHub / Telegram / Discord!