Afen

r2 plugin to rename expressions

Adam "satk0" Satko

r2con2024

Who am I?

- Student at Rzeszów University of Technology in Poland
- Small contributor to radare2 project

Limitation of afvn

afvn - can only rename **variables**!!!

What are the expressions?

I could bring up some smart definition here but they are just everything that resolves to a value (including **variables**).

Example expressions:

- $1 + 10$
- $2.4 * 0x10 * x$

... But afen can also rename instruction! (**push**, **jmp**, etc.)
So, it can rename **almost** everything!

Setup r2 with afen plugin

To setup afen you simply have to install it via **r2pm**:

```
r2pm -ci r2afen
```

To run r2 with afen plugin run:

```
r2 -e asm.parser=afen -e asm.pseudo=true <file>
```

Example of possible renamings

afen str "rbp - 9"
afen str[i] "rbp + rax - 9"

NOTE: Spaces are important!!

Inner implementation

The plugin uses both **RCore** and **RParse** APIs.

fcnptr	renaming
0x1	rbp+3:**i**
0x2	edi:**str[i]**
⋮	⋮

Figure: Hash table with function pointer as a key and rename struct as a value

In practice

Going to my comfortable place... (terminal)

Ideas for the future

- Support more complex constructions (e.g. **ignoring spaces**)
- Getting ready for the RParse API to be refactored - this plugin is just a **playground** for what is yet to come ;)
- ? Your ideas? Let me know there: `https://github.com/satk0/r2-afen-plugin.git`

Figure: QR code to the repo

Thank you all!