r2wars - battle bots in shared memory

github.com/hanemile/r2wars
Programme gleichzeitig im selben Speicher ausführen: was könnte schon schiefgehen? Hier geht's um das wie und anschließend selber mal hands-on damit spielen. Wir schauen uns den Unterbau an, bauen eigene kleine Programme die dann gegenseitig versuchen sich zu überschreiben.

https://emile.space/blog/2020/10-10-r2wars/

radare2

```
; r2 --
[0x00000000]>
```

Evaluable Strings Intermediate Language (ESIL)

```
4,esp,-=,ebp,esp,=[4]
```

```
esp -= 4
4bytes(dword) [esp] = ebp
```

Emulation

```
[0x00000000]> aei      # initialize ESIL VM state
[0x00000000]> aeim     # initialize ESIL VM stack
[0x00000000]> aer      # handle ESIL registers
[0x00000000]> aer PC=0x0      # set the Program Counter
[0x00000000]> aer PC=0x0      # set the StackPointer
```

r2wars

github.com/hanemile/r2wars

In diesem Workshop geht es um r2wars: dabei werden in geteiltem speicher zwei Programme gleichzeitig (mehr dazu im workshop) ausgeführt mit dem Ziel sich gegenseitig zu überschreiben. Es wird eine Einführung in das "wie geht das mit dem 'gleichzeitig' ausführen?" geben, dann bauen wir so bots und dann lassen wir sie alle gegeneinander antreten.

Ihr braucht:

– Einen Laptop
– radare2
– golang

```
; git clone github.com/hanemile/r2wars
; cd r2wars
```

```
; nix develop
```

```
; CGO_ENABLED=0 go run ./... -t 1s -v ./bots/warrior0.asm ./bots/warrior1.as
```

https://emile.space/blog/2020/10-10-r2wars/

---

https://github.com/hanemile/r2wars

@hanemile@chaos.social