GDB baby step 4

Medium Reverse Engineering picoGym Exclusive x86_64

AUTHOR: LT 'SYREAL' JONES

Description

`main` calls a function that multiplies `eax` by a constant. The flag for this challenge is that constant in decimal base. If the constant you find is 0x1000, the flag will be `picoCTF{4096}`.

Debug this.

Hints

1

Buka dengan binary ninja.

```
int32_t main(int32_t argc, char** argv, char** envp)

    int32_t argc_1 = argc
    char** argv_1 = argv
    int32_t var_c = 0x28e
    int32_t var_10 = 0
    int32_t var_10_1 = func1(0x28e)
    return 0x28e
```

bisa kita lihat fungsi main terdapat fungsi internal yaitu func1(), kita cek saja apa algoritma yang ada pada func1.

```
uint64_t func1(int32_t arg1) __pure

    return zx.q(arg1 * 12905)
```

flag : picoCTF{12905}