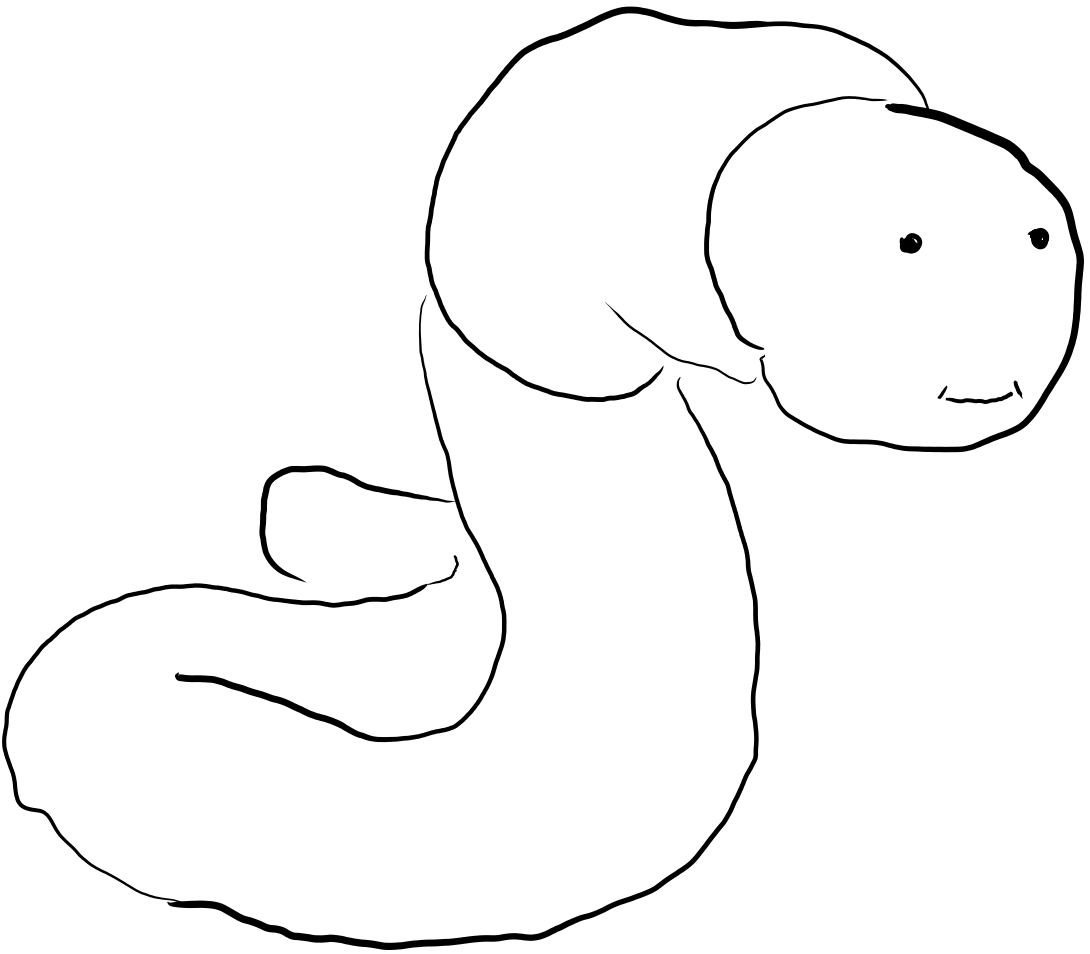


Nefarious

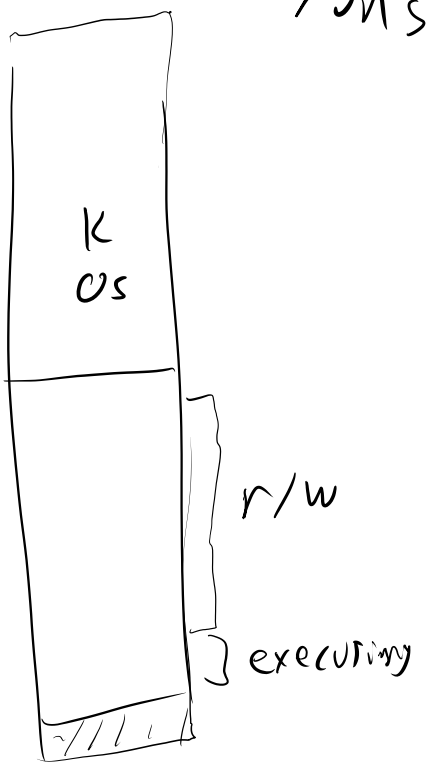
back door

buffer overflow

arbitrary power

read ____

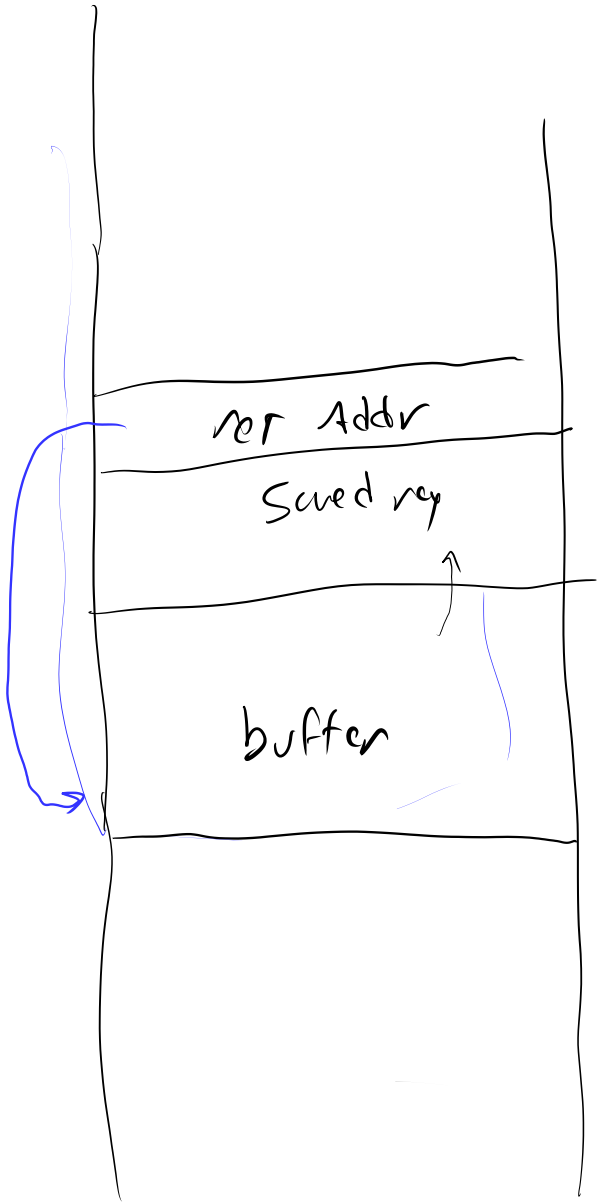
runs what was read



ASLR

Address space layout randomization

Stack




```
char buf[256];
scanf("%s", buf);
```

buffer overflow vulnerability

255

256

0x0 code 0 ... 0x0 add

find vulnerability by them; then:

tell them collect bounty

Publish, be famous

copy code, fix it, sell it

tell them & someone & start bidding war

sell to NSA

tell them

tell them, wait, become a bad guy

exploit, get bored, tell them

ignore

tell them, wait, publish

find vulnerability by them; then:

tell them collect bounty

Publish, be famous

copy code, fix it, sell it

tell them & someone & start bidding war

sell to NSA

tell them

tell them, wait, become a bad guy

exploit, get bored, tell them

ignore

tell them, wait, publish

functions

```
foo:
    ...
```

```
int foo(int x, code addr y){
    ...
    call y
}
```

```
movq $3, %rdi
callq foo
```

```
foo(3)
```

Overloading – same name, diff sig

Overriding – same name, diff between
base & diff class