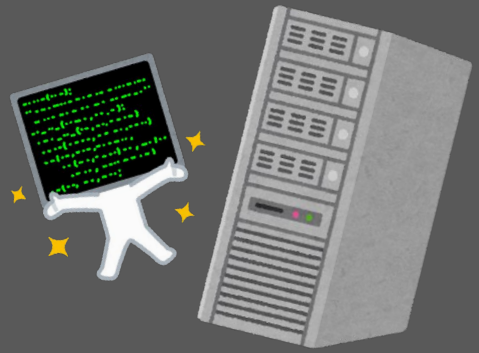
containers / security / a fun time

pick two

Aleksa (cyphar)


who’s heard of containers?

let's build a website!




```
/
├
├
├
├
└── var
    ├
    ├
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```


```
/
├
│
│
│
│
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
/
├
├
├
├
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
/
├── etc
│   └── shadow
│
│
│
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Can I `GET files/music.mp3`?

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Can I `GET files/music.mp3`?

Hmm, where is `files/music.mp3`?

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Can I `GET files/music.mp3`?

Ah, here it is!

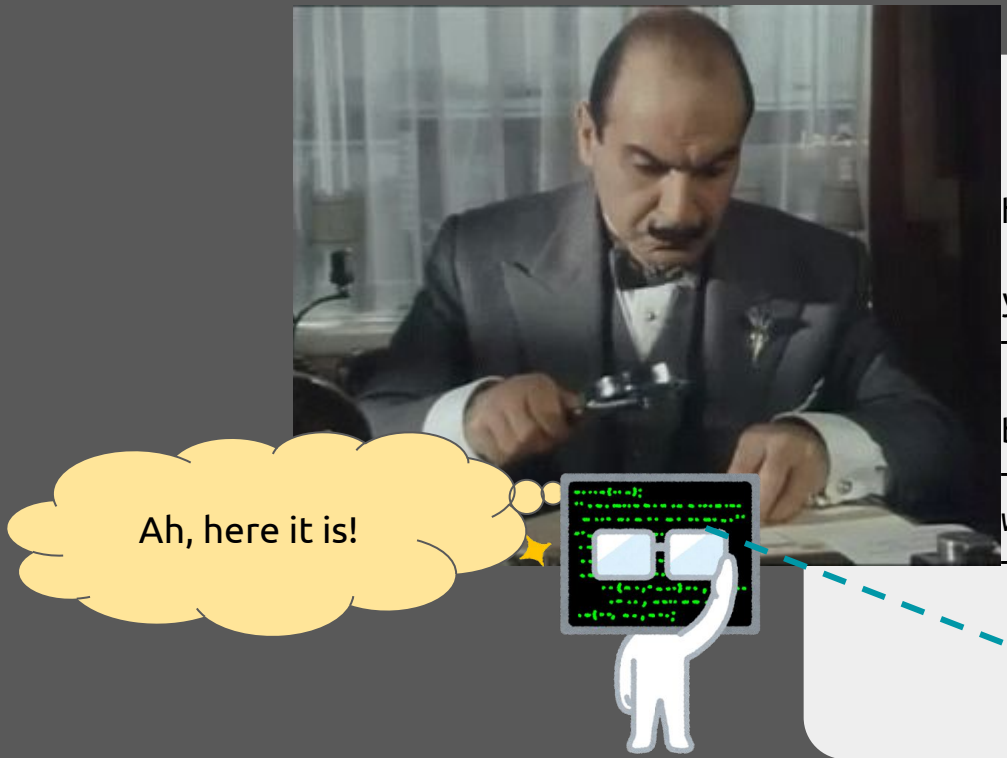
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Can I GET files/music.mp3?

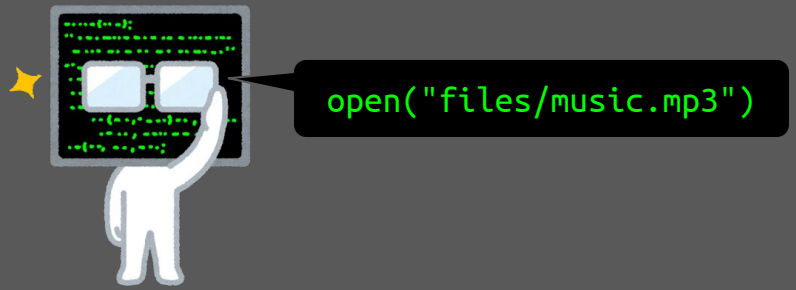
Here you go!

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

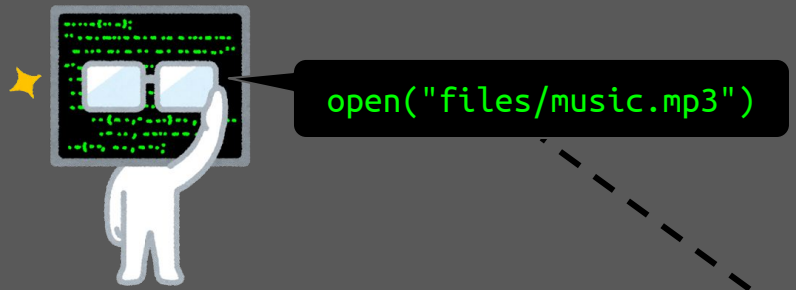

```
hadow

yphar
└── secrets.txt

b
└── userdata
ww
└── htdocs
    ├── index.html
    └── files
        └── music.mp3
```



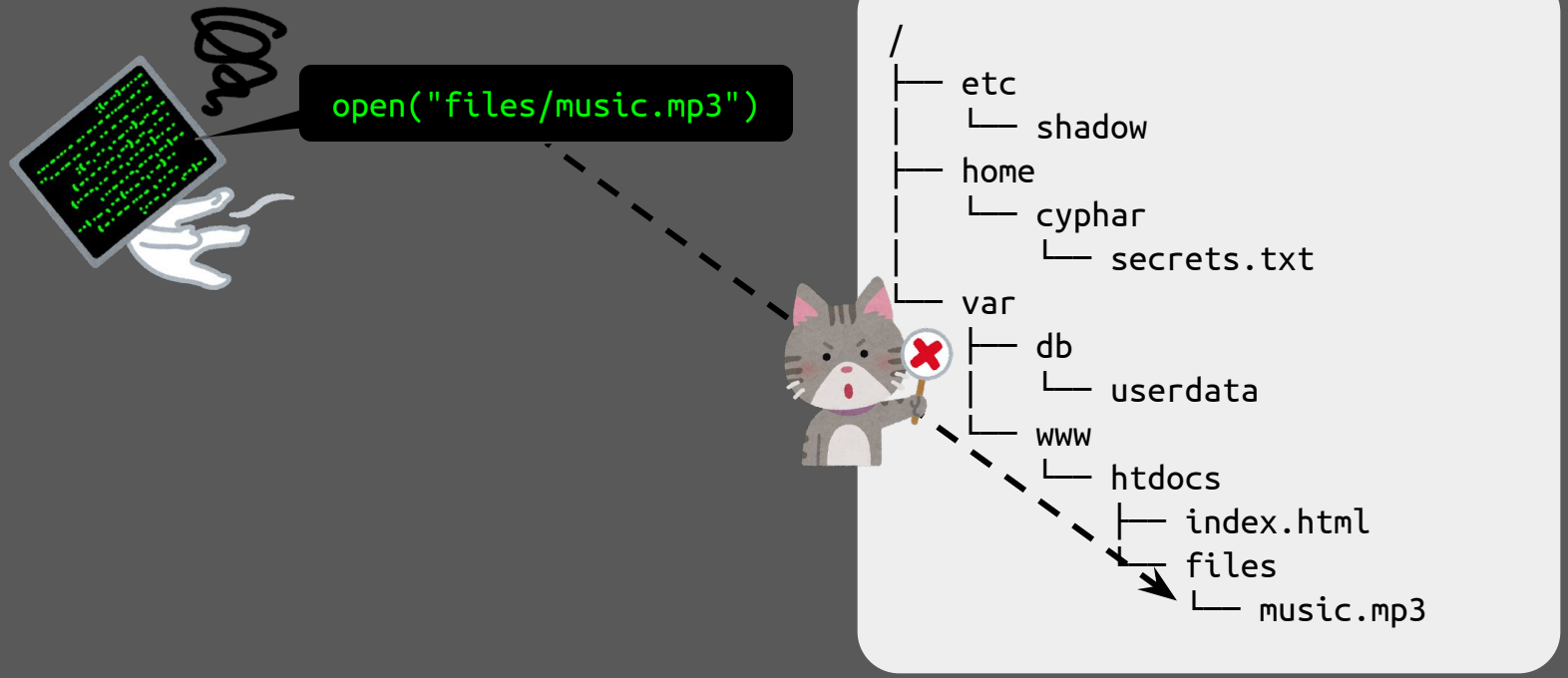

```
hadow

yphar
── secrets.txt

b
── userdata
ww
── htdocs
   ├── index.html
   └── files
       └── music.mp3
```



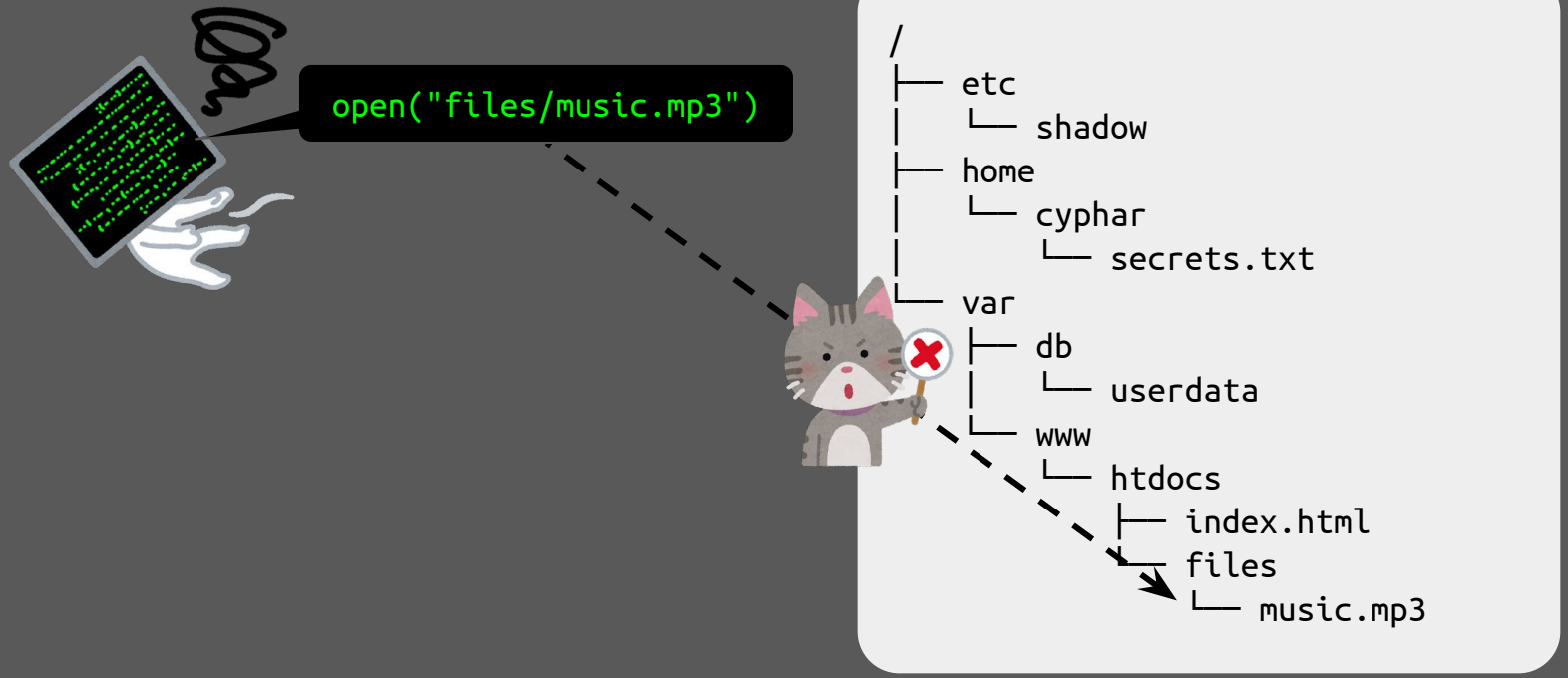

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

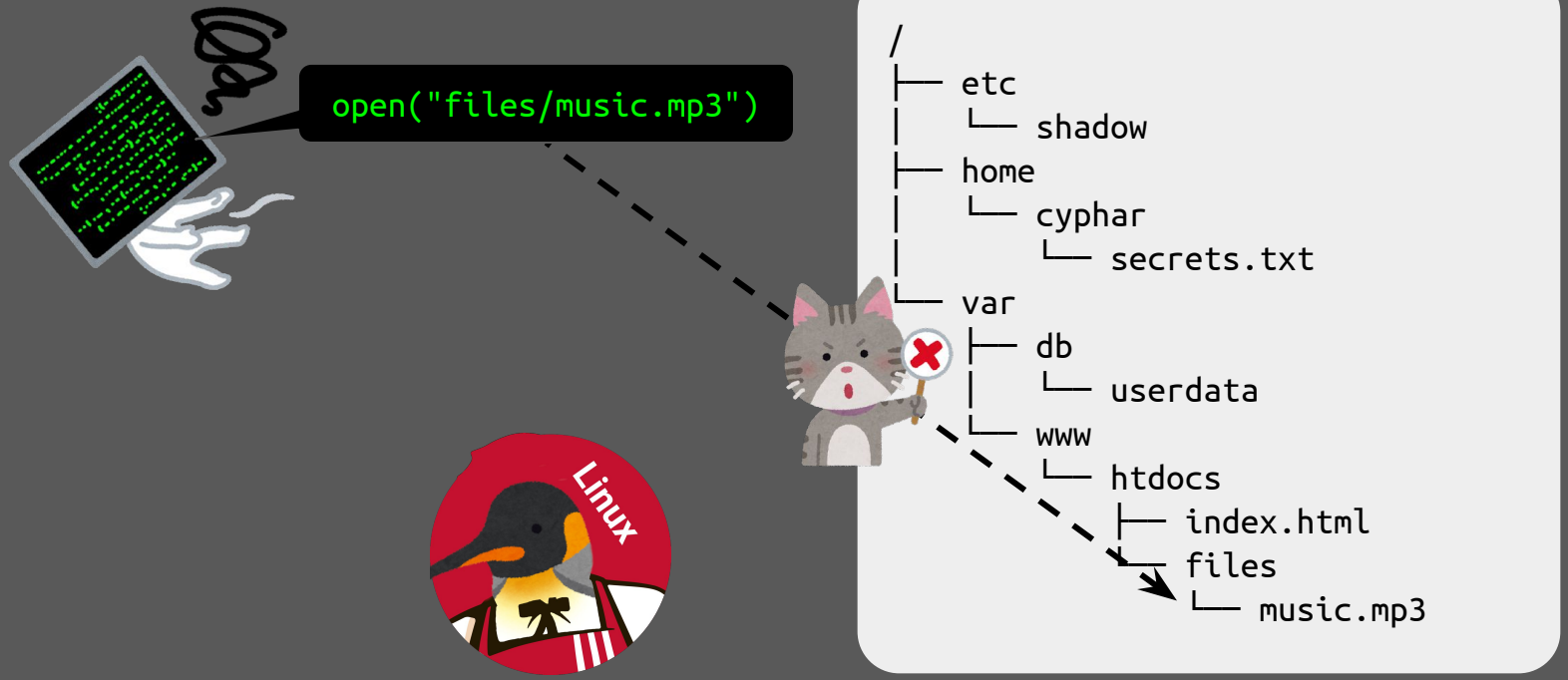



```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```


open("files/music.mp3")
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3

it’s all about the kernel!


open("files/music.mp3")
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


open("files/music.mp3")
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3
Linux

the kernel provides

abstractions

the kernel provides

abstractions

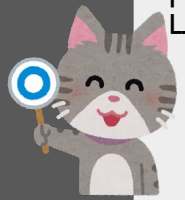
(among other things)

```
open("files/music.mp3")
```

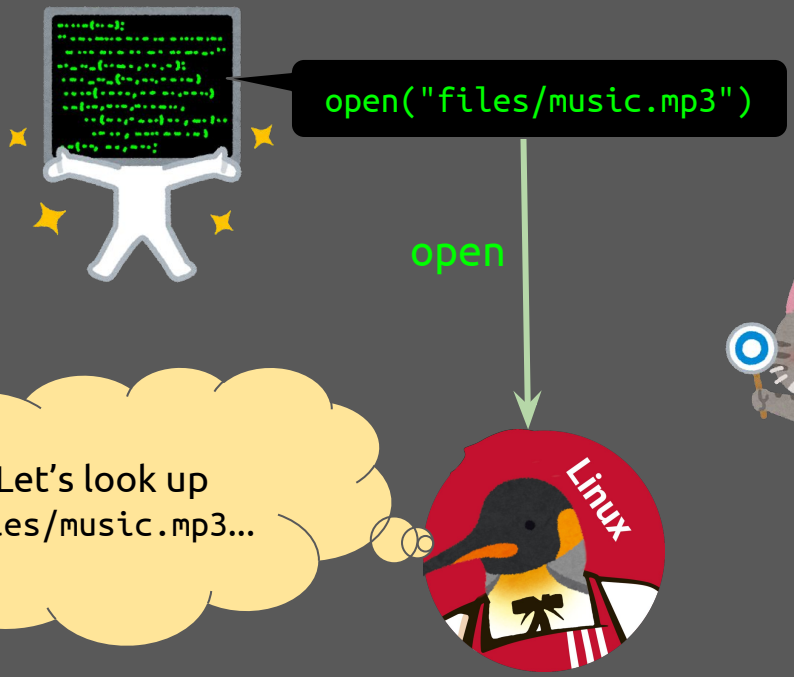

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

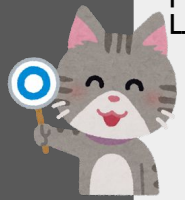
open("files/music.mp3")

open

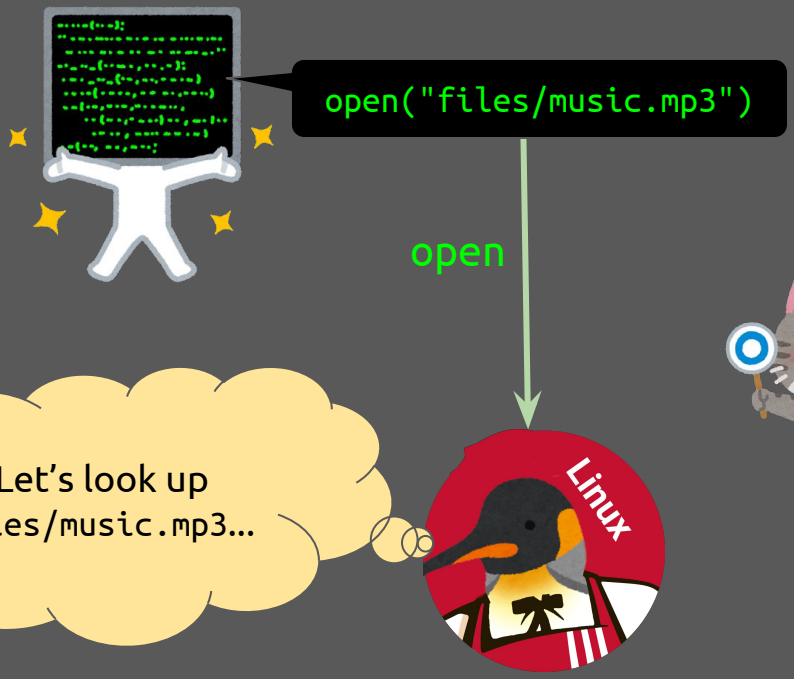


```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```





```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```



./files/music.mp3

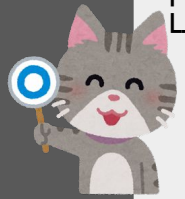
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

open("files/music.mp3")

open

Let's look up
files/music.mp3...

./files/music.mp3



```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

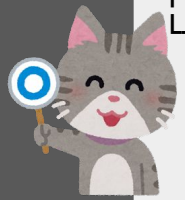
open("files/music.mp3")

open

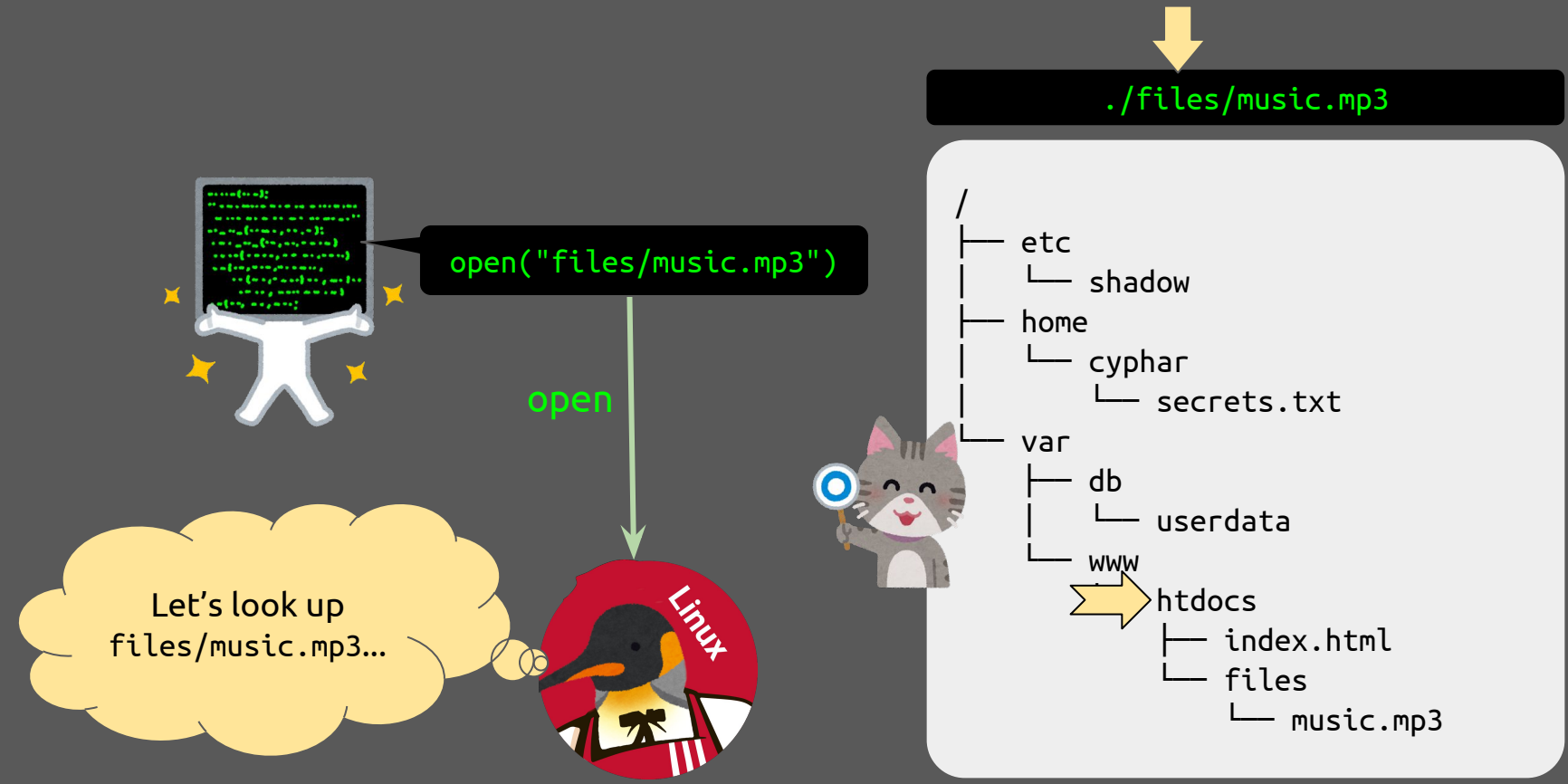
Let's look up files/music.mp3...

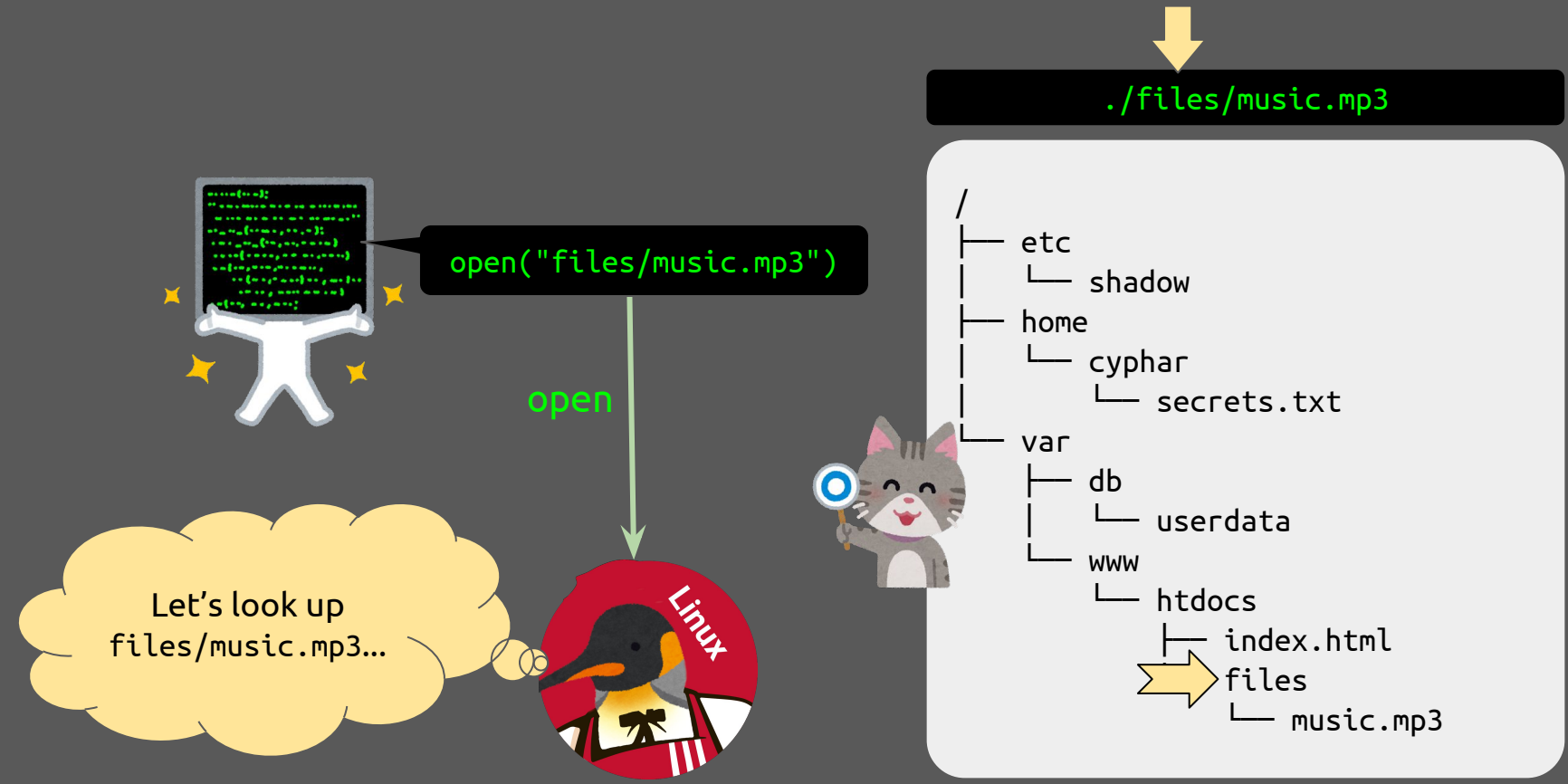
Program's working directory is /var/www/htdocs.

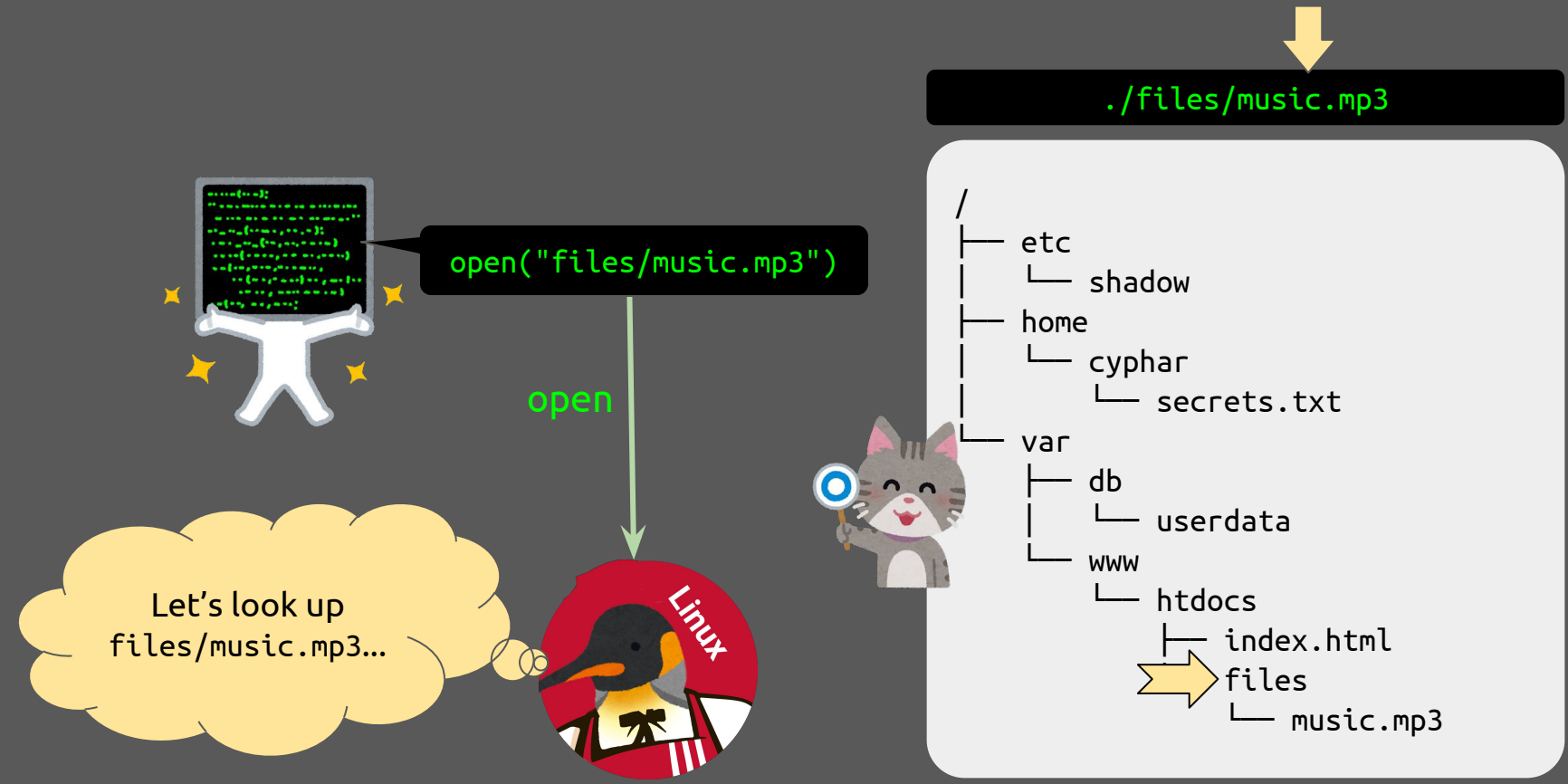
./files/music.mp3

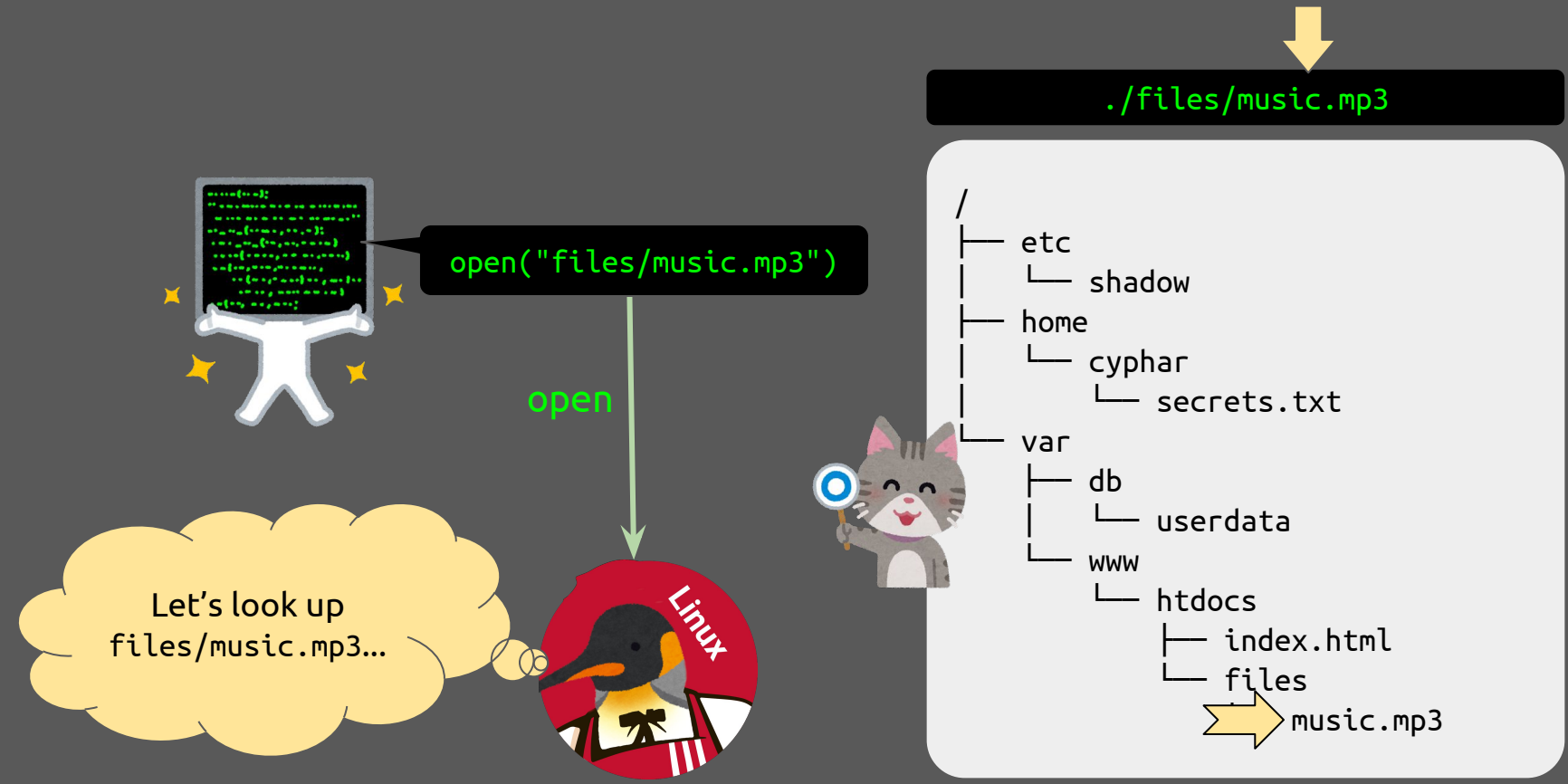


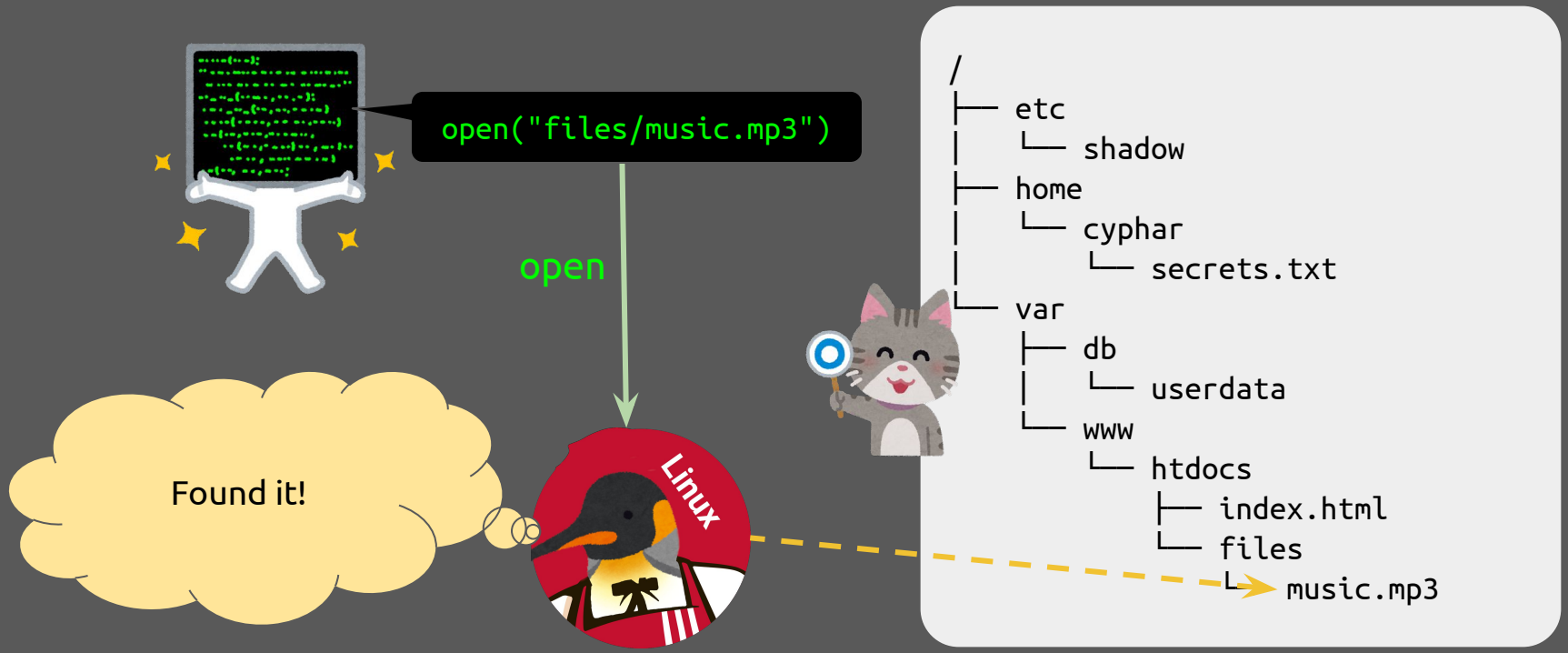
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

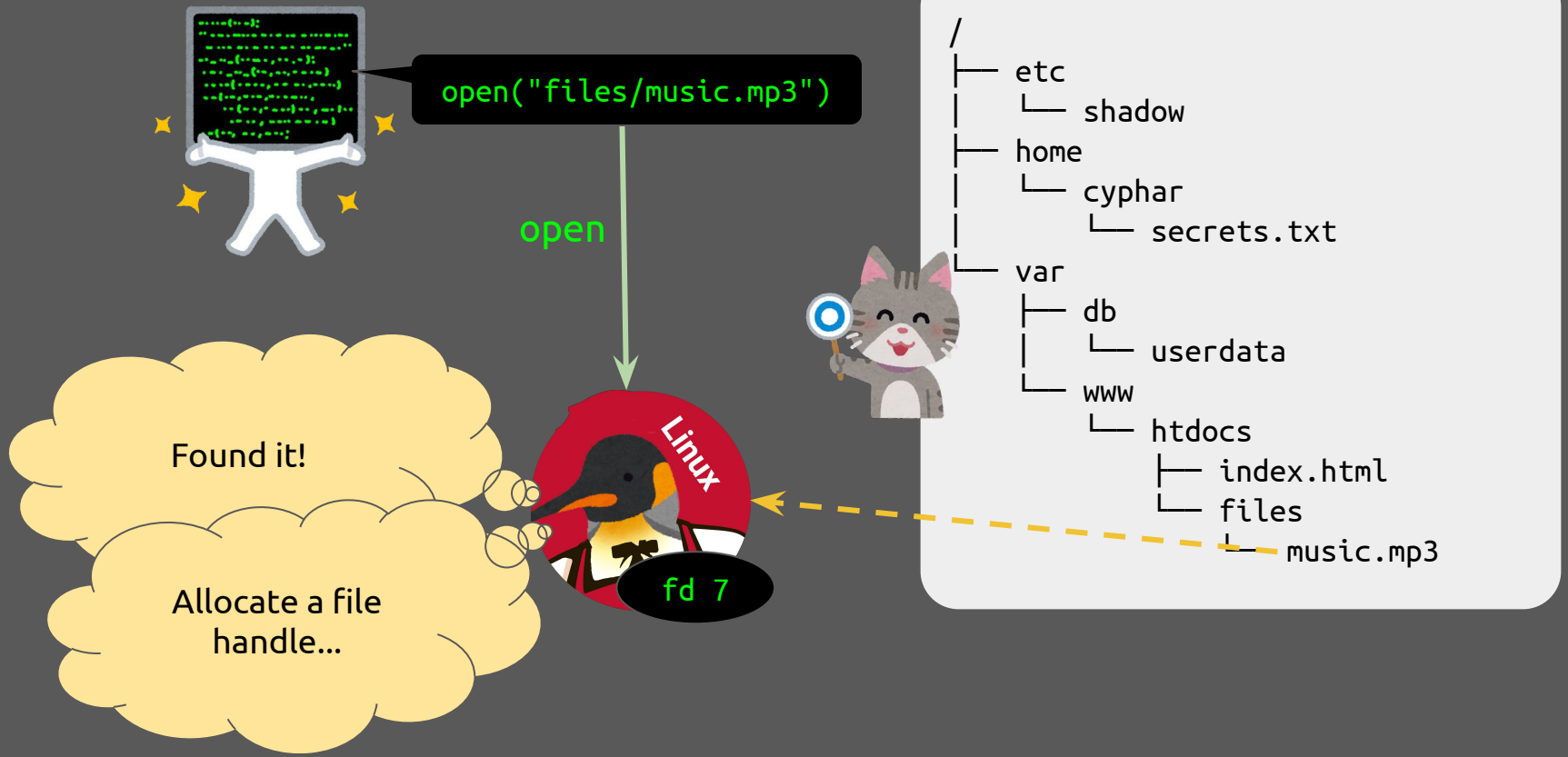

./files/music.mp3
open("files/music.mp3")
open
Let's look up
files/music.mp3...
Linux
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


./files/music.mp3
/
├── etc
│ └── shadow
├── home
│ └── cyphar
│ └── secrets.txt
└── var
├── db
│ └── userdata
└── www
└── htdocs
├── index.html
└── files
└── music.mp3
open("files/music.mp3")
open
Let's look up
files/music.mp3...
Linux


./files/music.mp3
open("files/music.mp3")
open
Let's look up
files/music.mp3...
Linux
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


./files/music.mp3
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3
open("files/music.mp3")
open
Let's look up
files/music.mp3...
Linux


open("files/music.mp3")
open
Found it!
Linux
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


open("files/music.mp3")
open
Found it!
Allocate a file handle...
Linux
fd 7
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Wow, that was easy!


Linux
fd 7


I made this.
Linux
fd 7

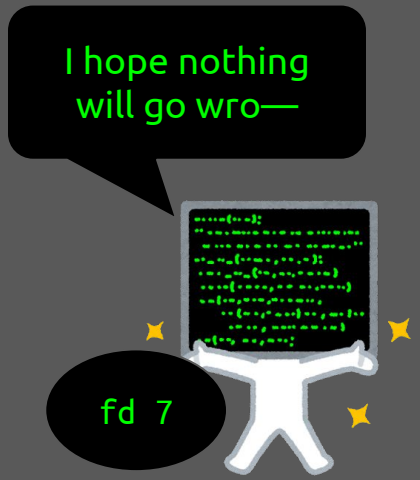

I made this.
You made this?
Linux
fd 7


Linux


fd 7


fd 7


I made this.
fd 7

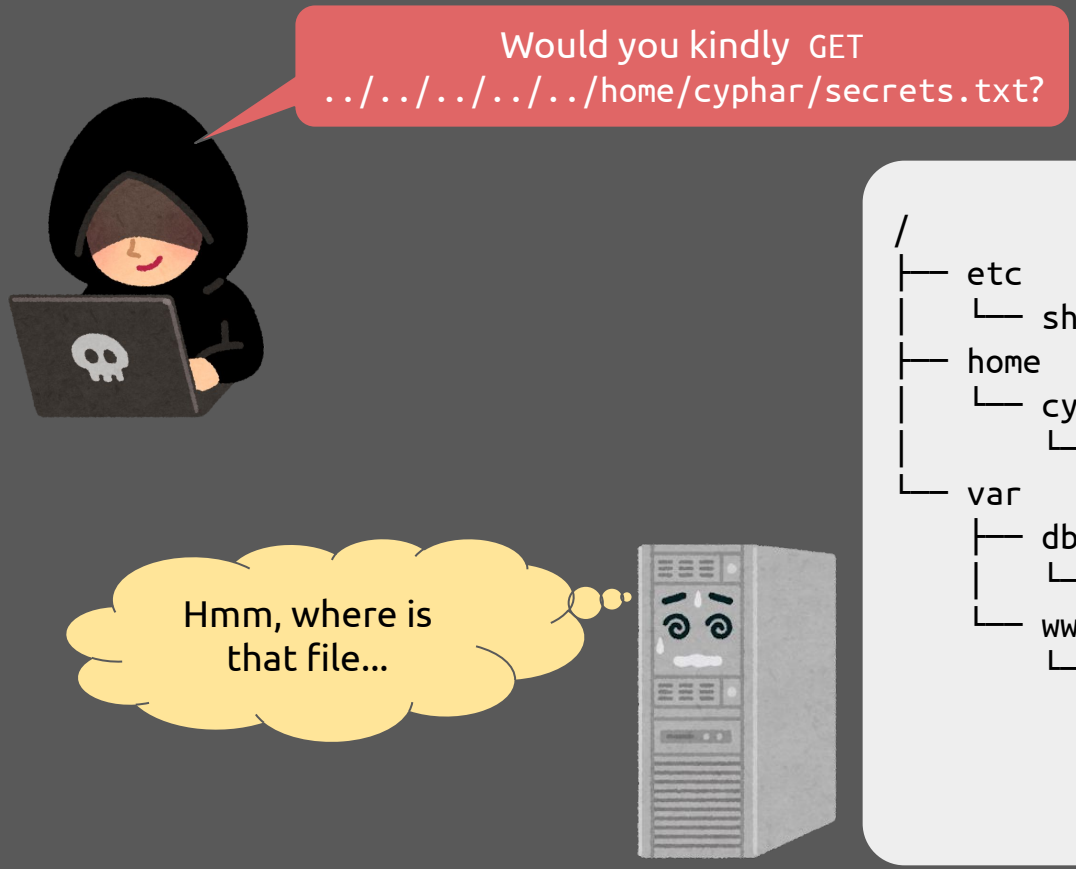

I hope nothing will go wro—
fd 7

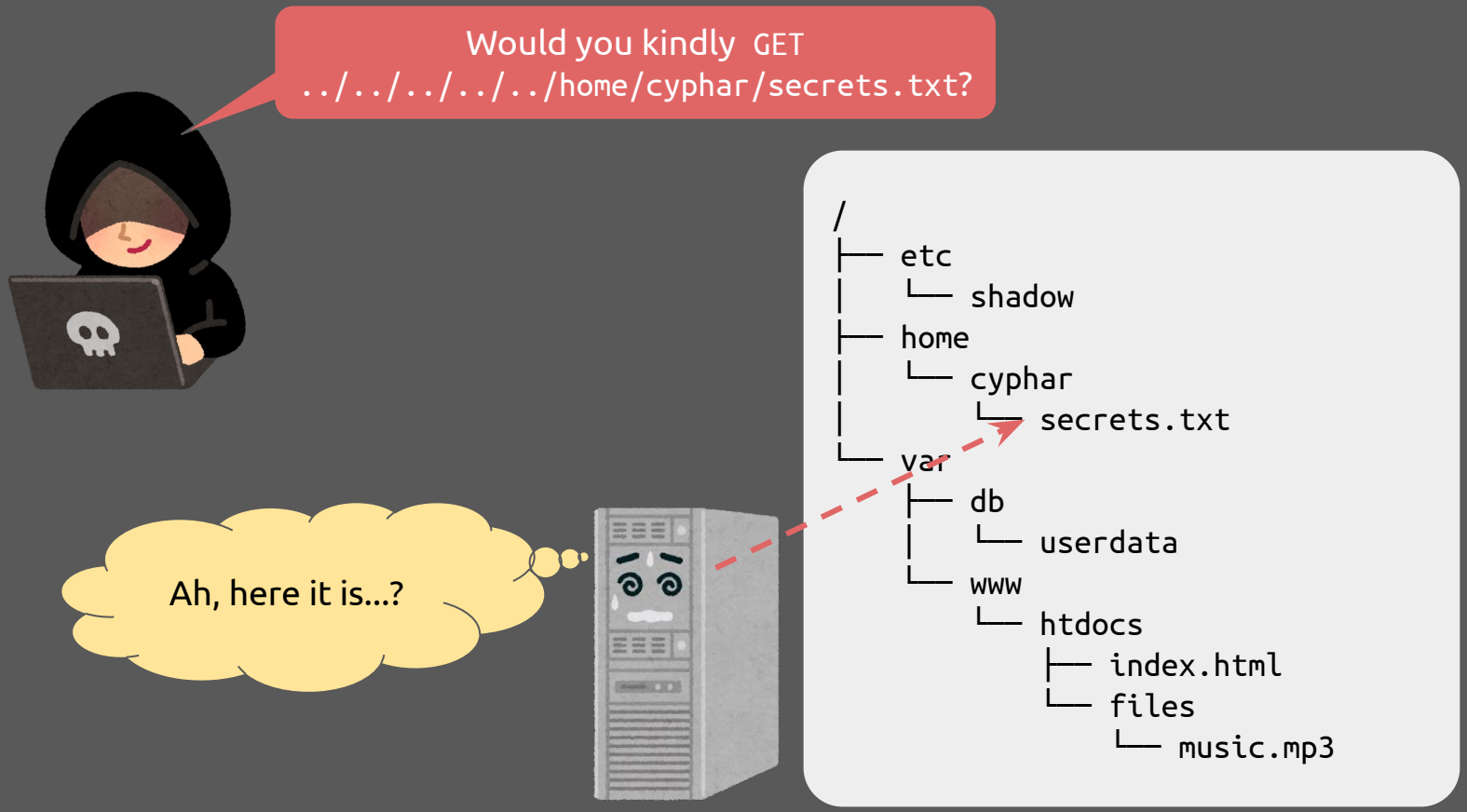

A new foe has appeared!
CHALLENGER APPROACHING

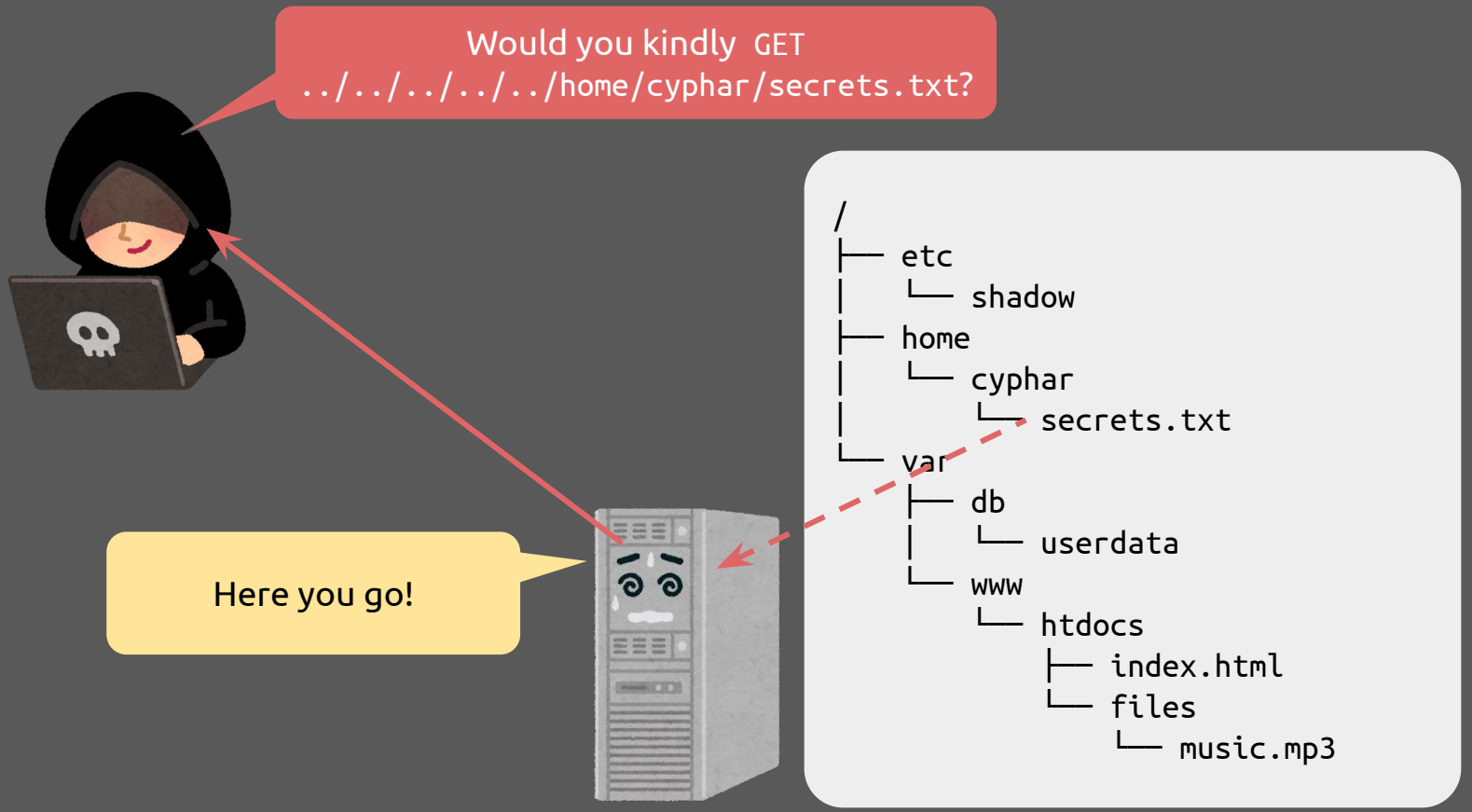
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Would you kindly `GET`
`../../../../../home/cyphar/secrets.txt`?

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```


Would you kindly GET
../../../../../home/cyphar/secrets.txt?
Hmm, where is that file...
/
├── etc
│ └── shadow
├── home
│ └── cyphar
│ └── secrets.txt
└── var
├── db
│ └── userdata
└── www
└── htdocs
├── index.html
└── files
└── music.mp3


Would you kindly GET
../../../../../home/cyphar/secrets.txt?
Ah, here it is...?
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3


Would you kindly GET
../../../../../home/cyphar/secrets.txt?
Here you go!
/
etc
shadow
home
cyphar
secrets.txt
var
db
userdata
www
htdocs
index.html
files
music.mp3

```
open("../../../../../home/cyphar/secrets.txt")
```

open


```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
../../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up ../../../../../ home/cyphar/ secrets.txt...

Program's working directory is /var/www/htdocs.


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
../../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
../../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
../../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up ../../../../../ home/cyphar/ secrets.txt...

Okay, we've hit the root and can't go further.


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up ../../../../../ home/cyphar/ secrets.txt...

Okay, we've hit the root and can't go further.


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
../../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
open("../../../../../home/cyphar/secrets.txt")
```

open

Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

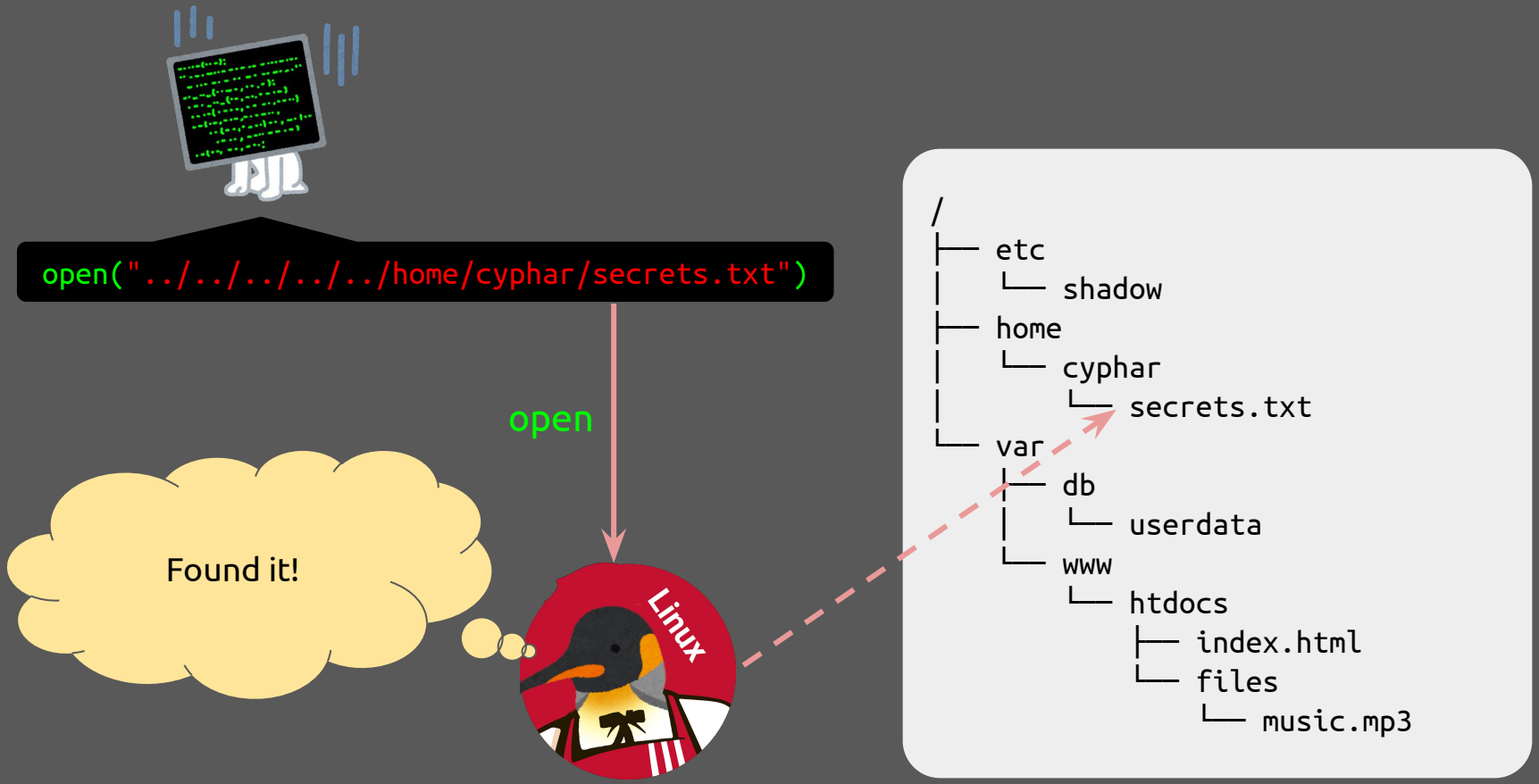
```
open("../../../../../home/cyphar/secrets.txt")
```

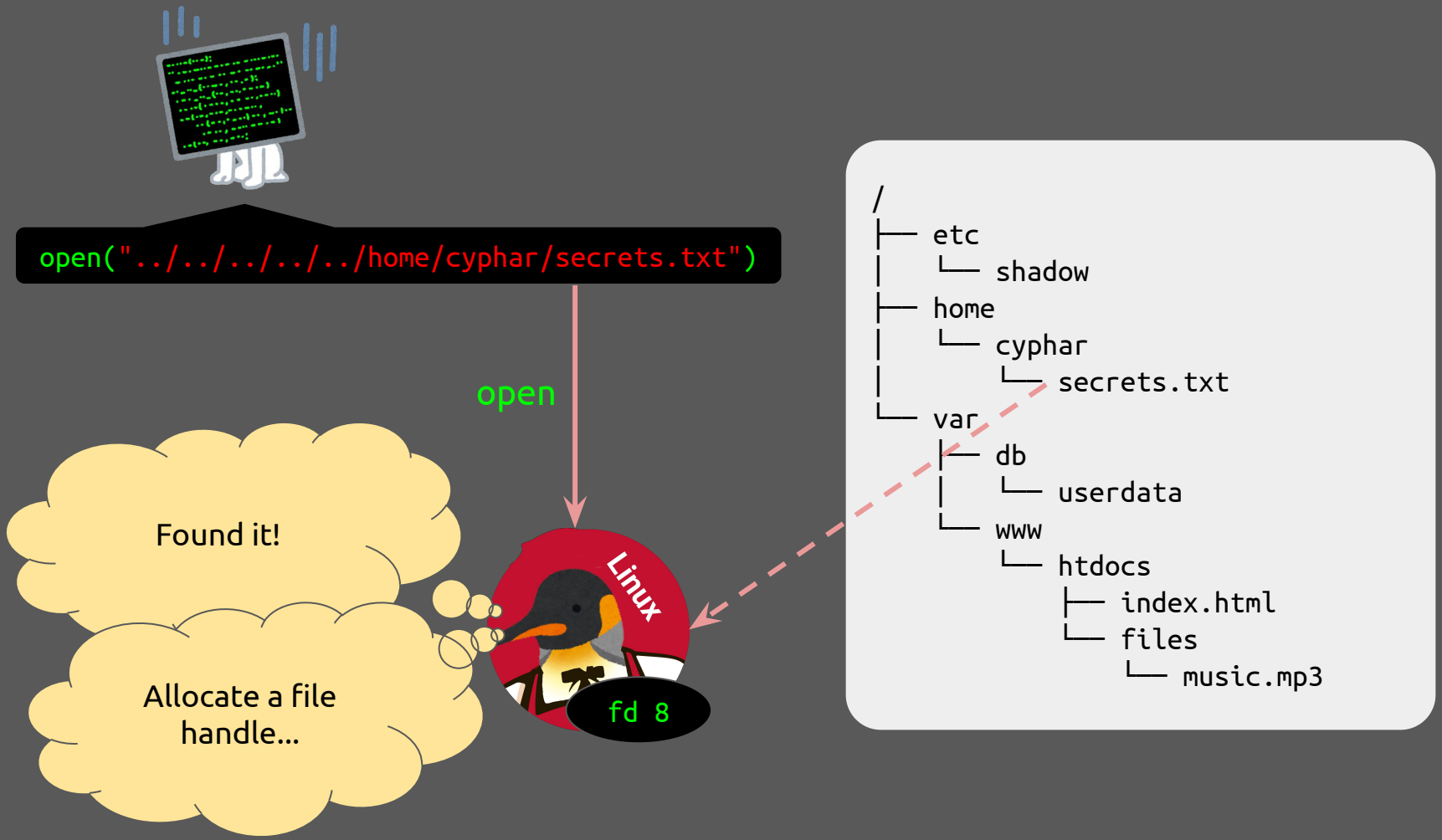
open

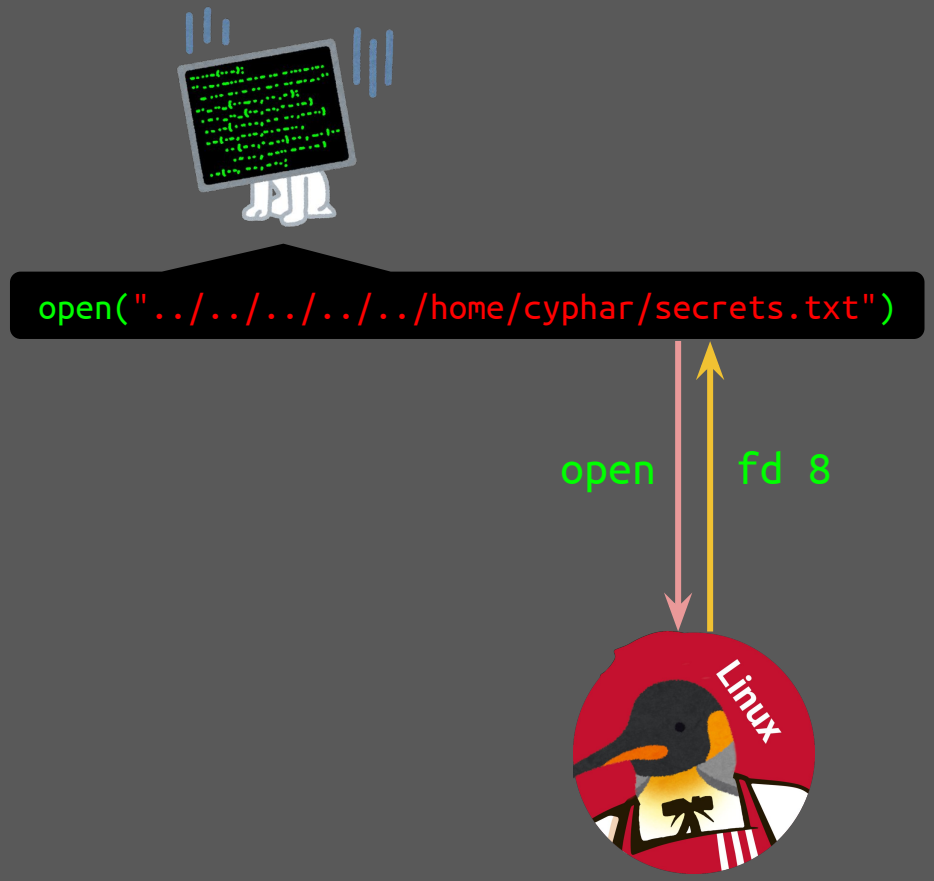
Let's look up
../../../../../
home/cyphar/
secrets.txt...


```
./../../../../../home/cyphar/secrets.txt
```

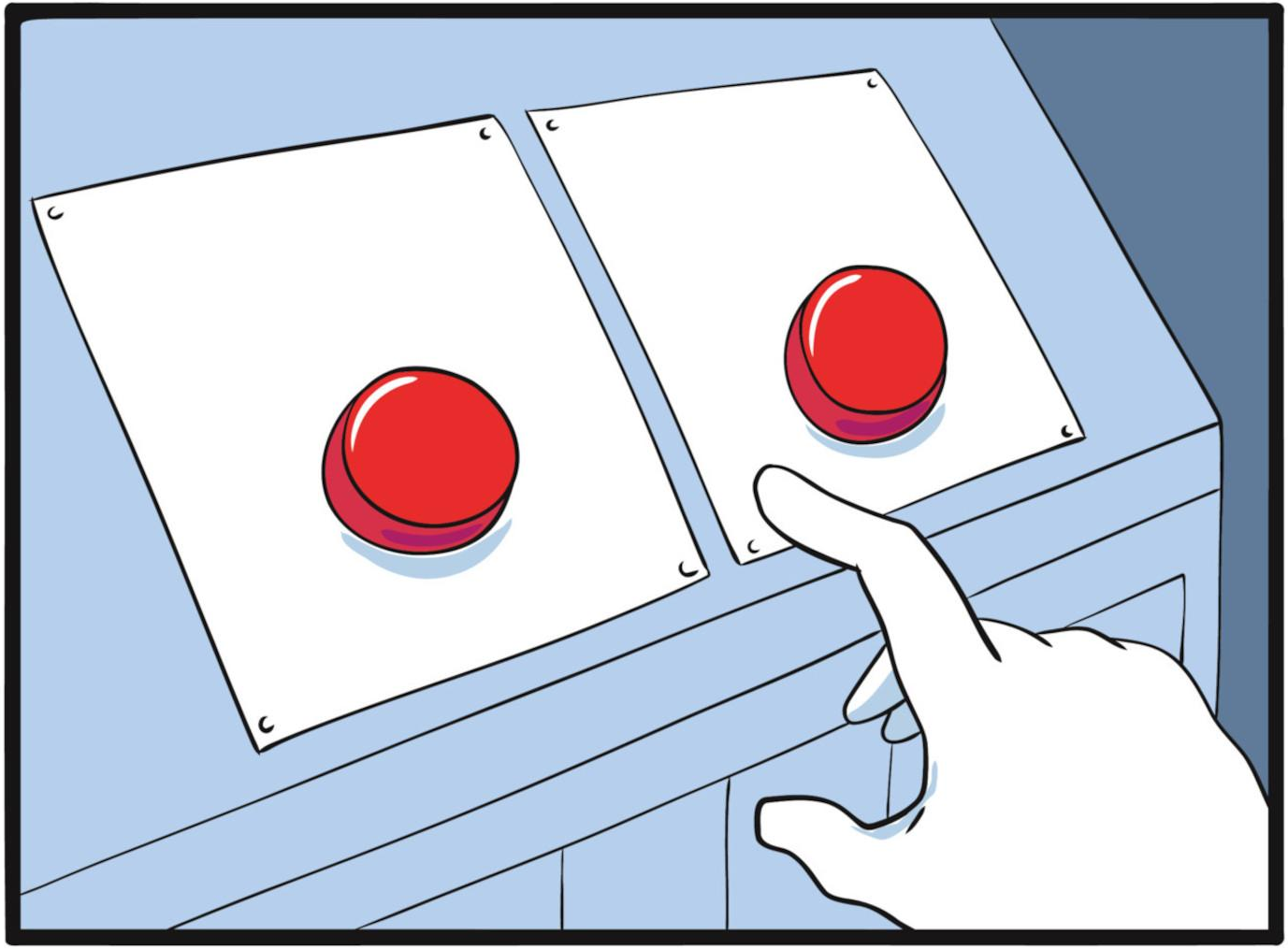
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```


open("../../../../../home/cyphar/secrets.txt")
open
Found it!
Linux
/
├── etc
│ └── shadow
├── home
│ └── cyphar
│ └── secrets.txt
└── var
├── db
│ └── userdata
└── www
└── htdocs
├── index.html
└── files
└── music.mp3


open("../../../../../home/cyphar/secrets.txt")
open
Found it!
Allocate a file handle...
Linux
fd 8
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│   └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3




```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```




“just write bug-free software”

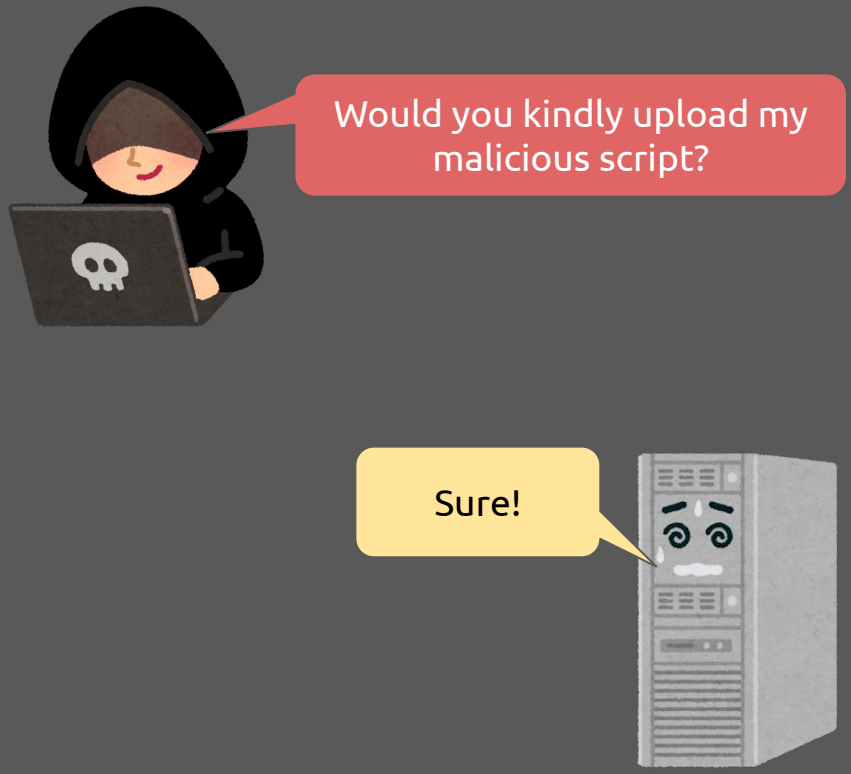
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

r2a

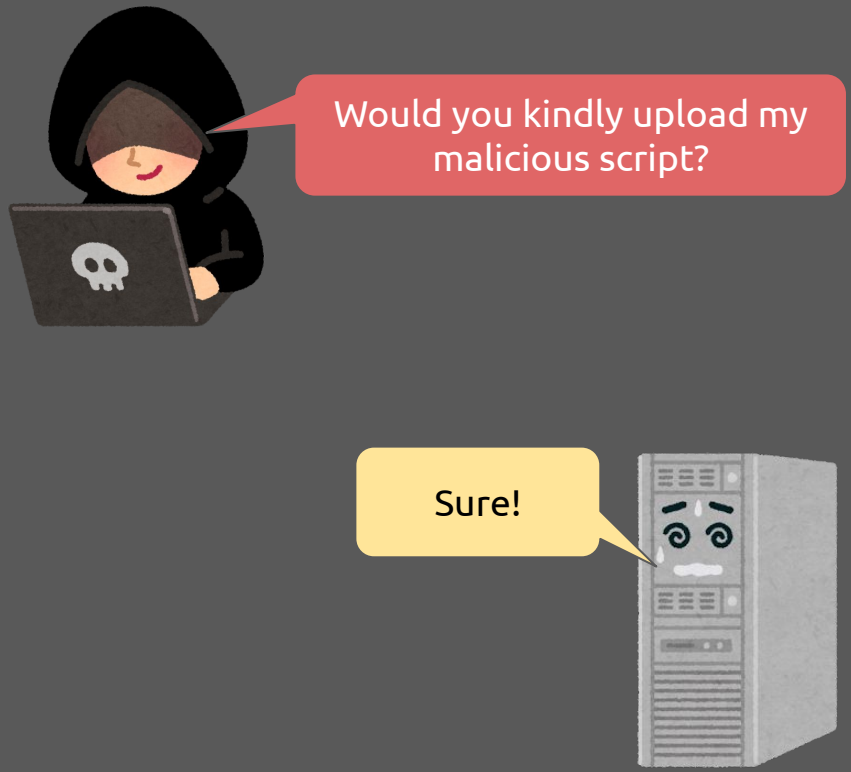
```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```




```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

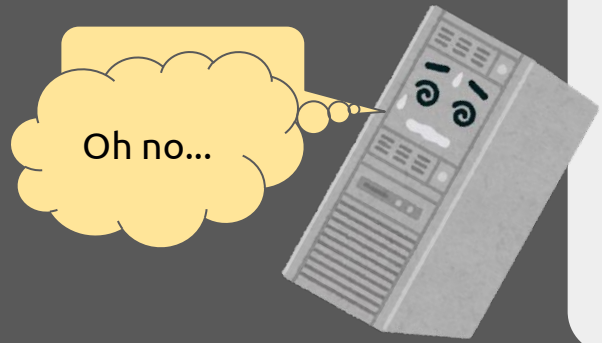

Would you kindly upload my malicious script?
Sure!
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── shell.php
            └── files
                └── music.mp3

Would you kindly run `shell.php`?

Sure!

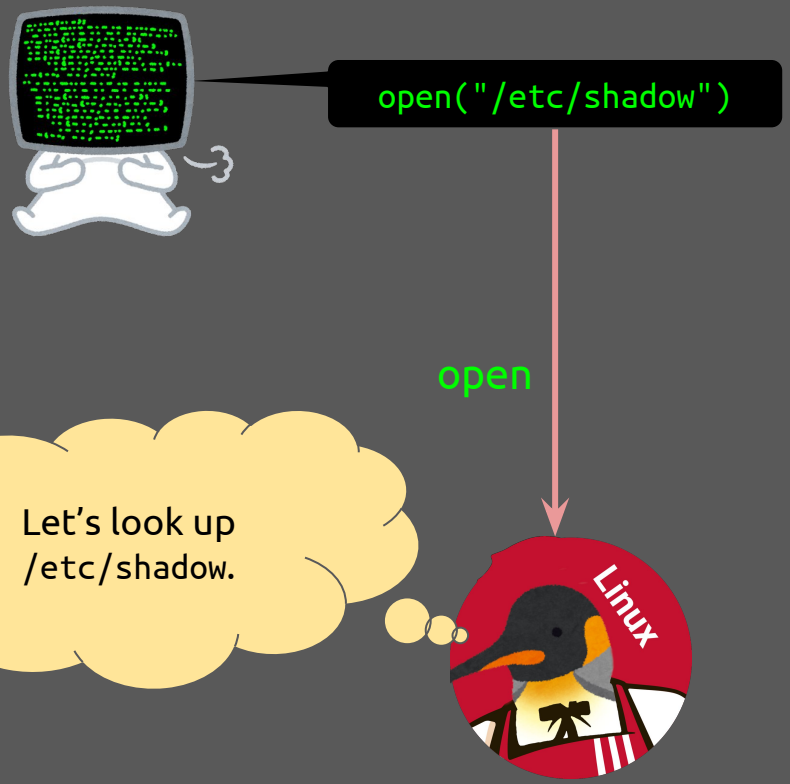
```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── shell.php
            └── files
                └── music.mp3
```

Would you kindly run `shell.php`?



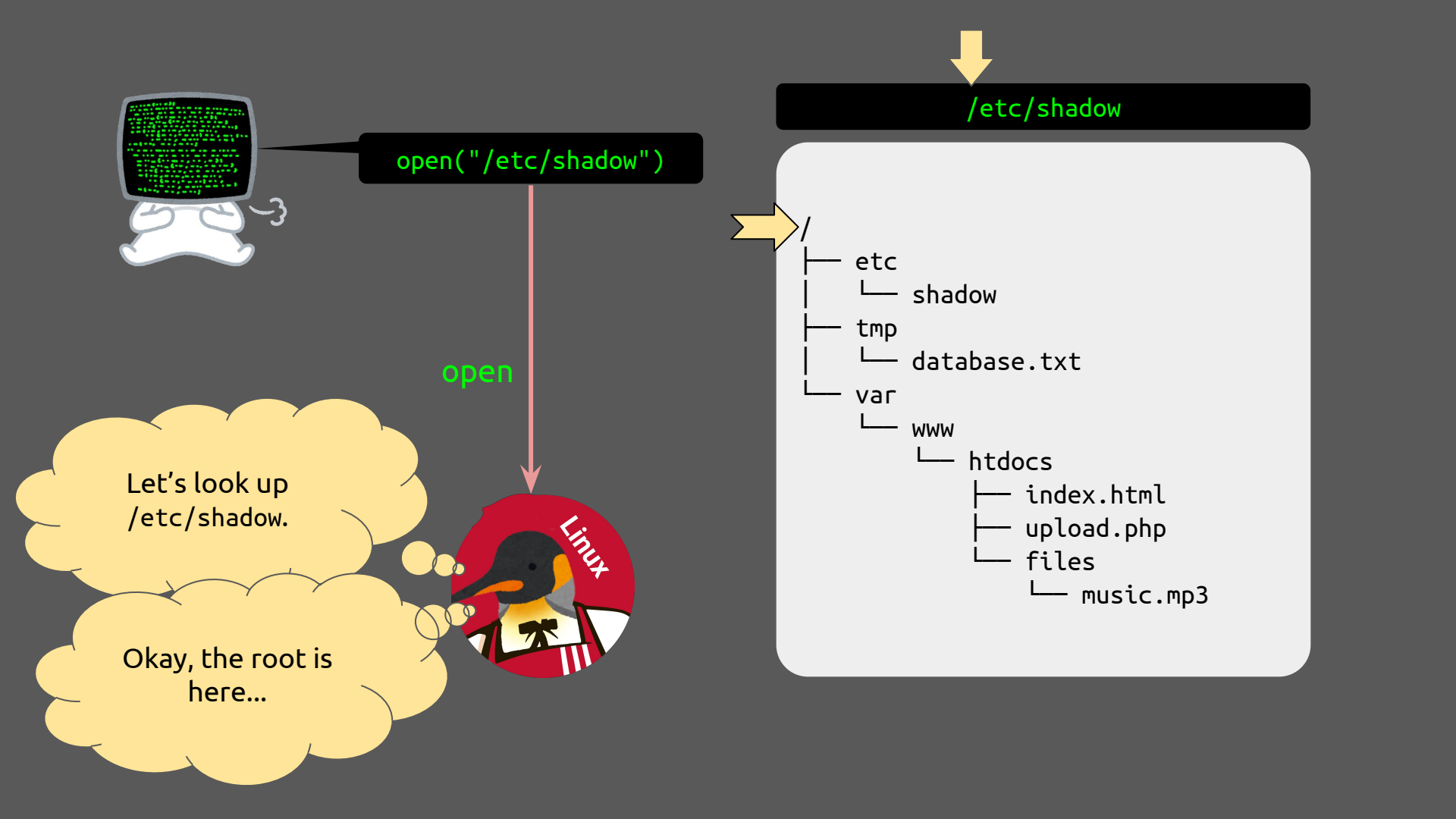

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── shell.php
            └── files
                └── music.mp3
```


“just lie”



/etc/shadow

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```


open("/etc/shadow")
/etc/shadow
open
Let's look up /etc/shadow.
Okay, the root is here...
Linux
/
├── etc
│ └── shadow
├── tmp
│ └── database.txt
└── var
└── www
└── htdocs
├── index.html
├── upload.php
└── files
└── music.mp3

open("/etc/shadow")

open

Let's look up /etc/shadow.

/etc/shadow

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

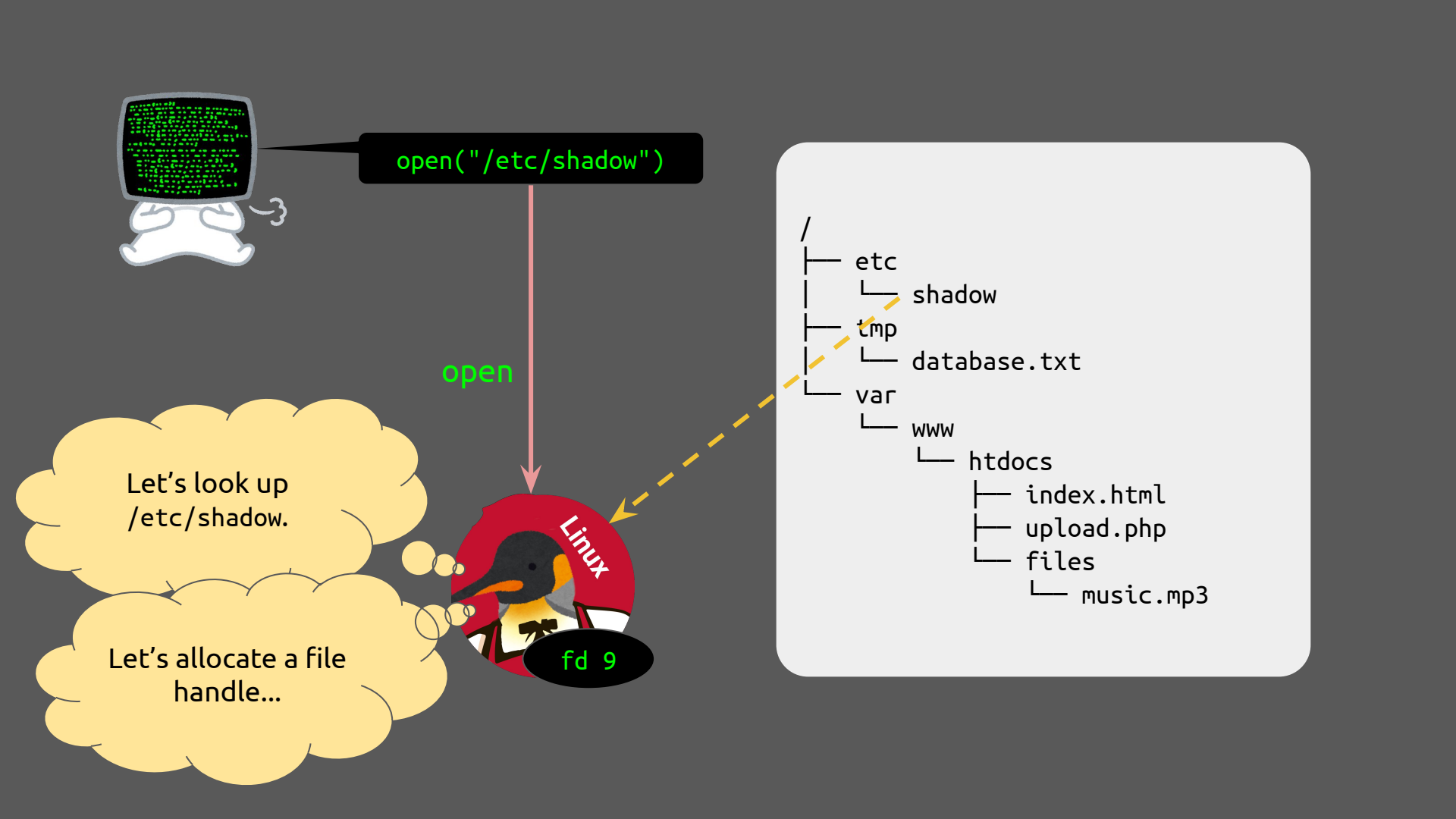
open("/etc/shadow")

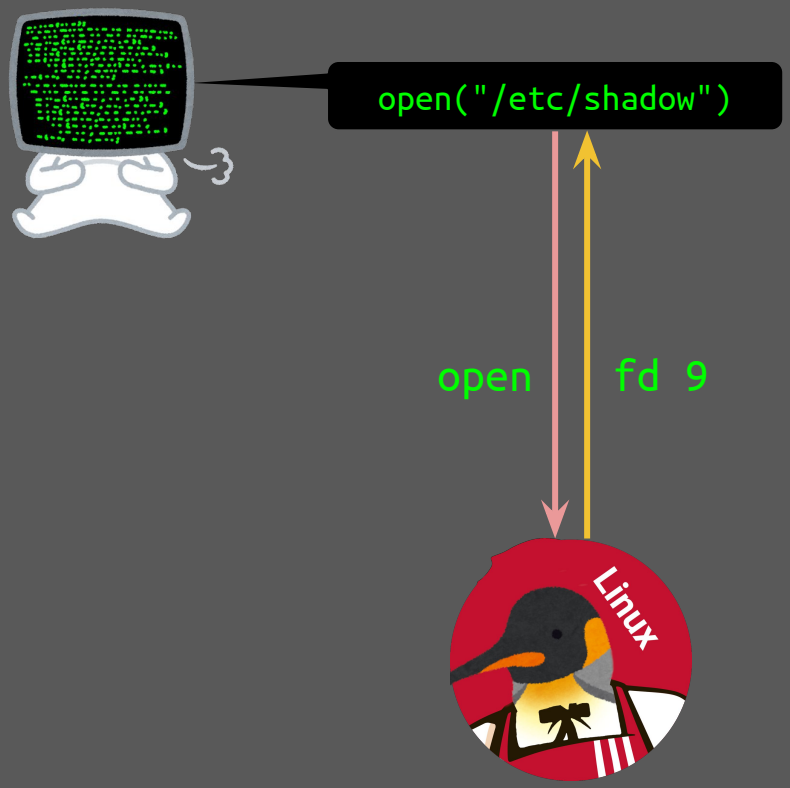
open

Let's look up /etc/shadow.

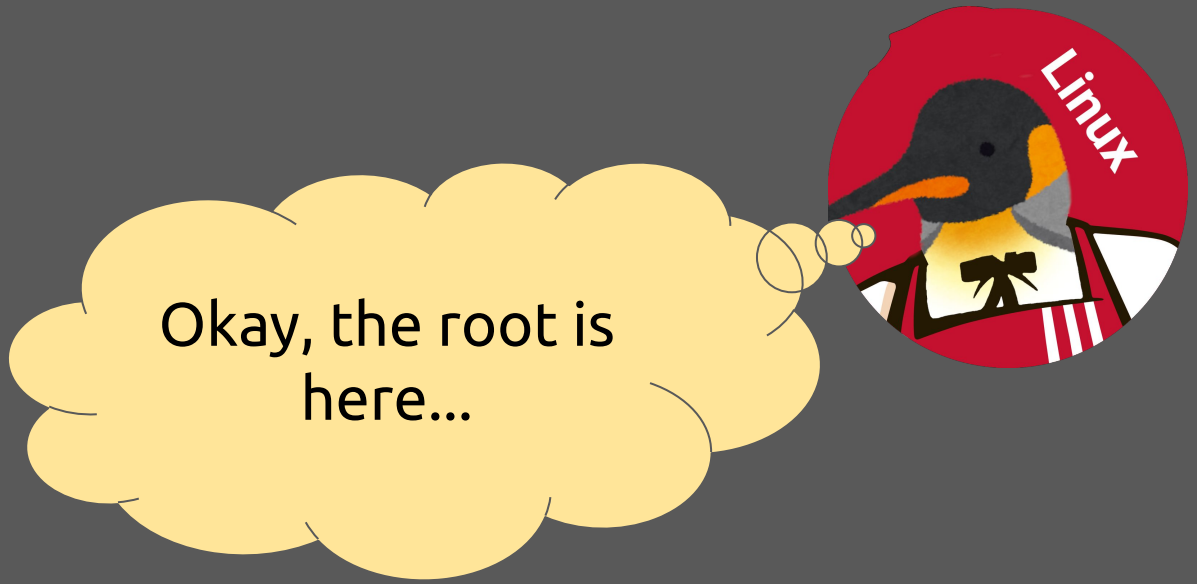
/etc/shadow

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

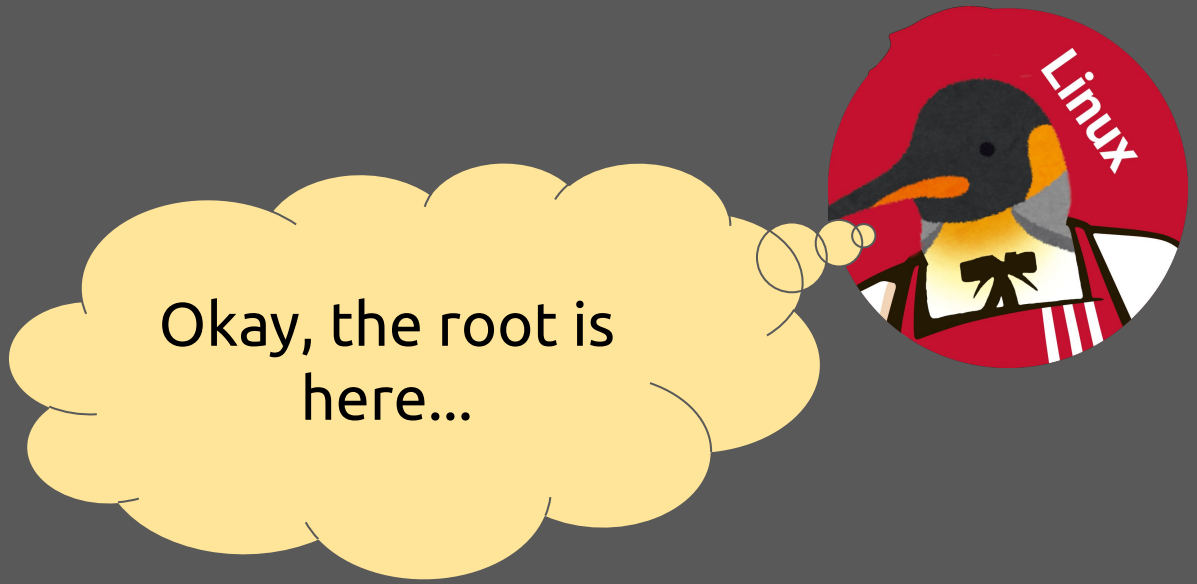

open("/etc/shadow")
open
Let's look up /etc/shadow.
Let's allocate a file handle...
Linux
fd 9
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3




```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

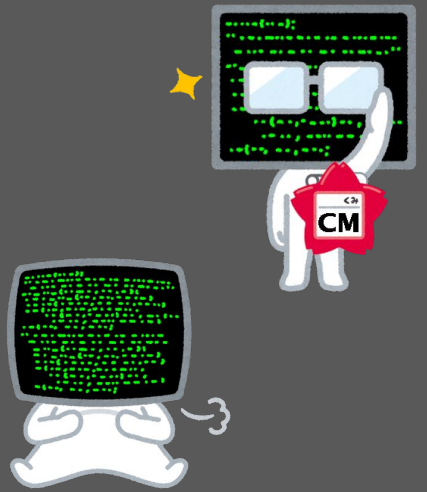

Linux
Okay, the root is here...


chroot

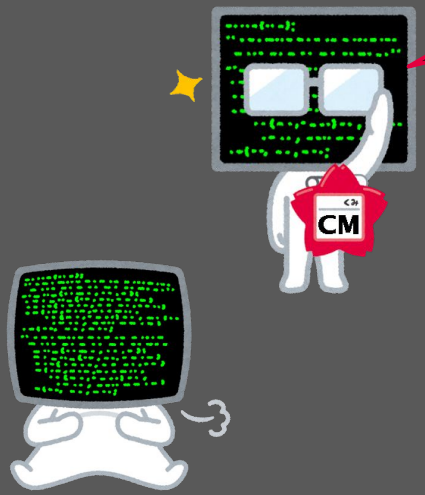

Linux
Okay, the root is here...


CM

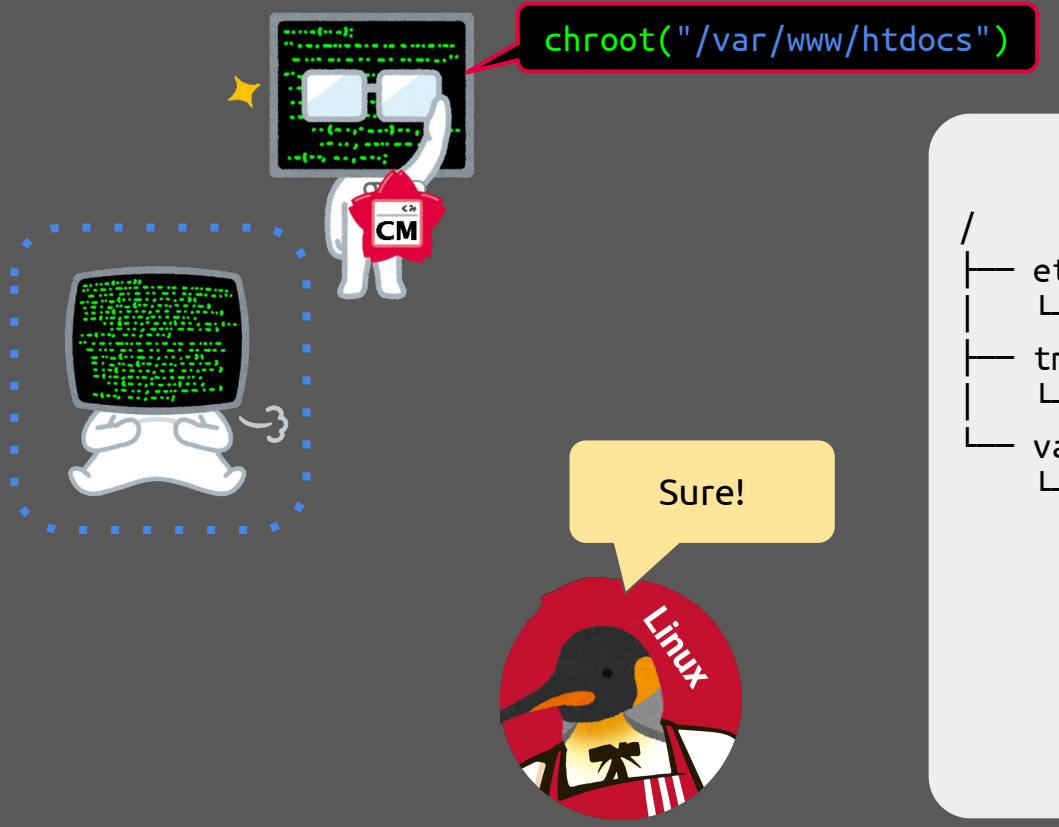
Container
Manager



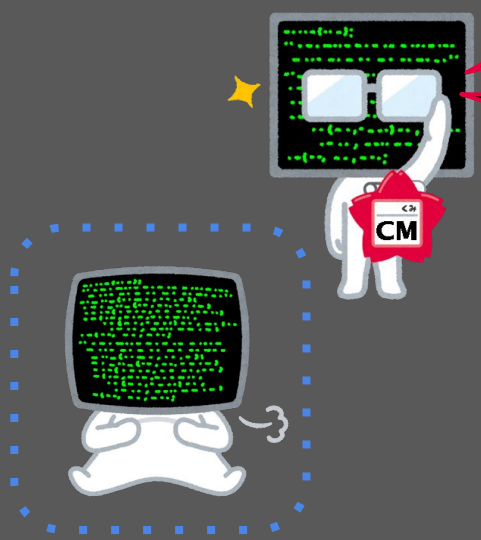

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```



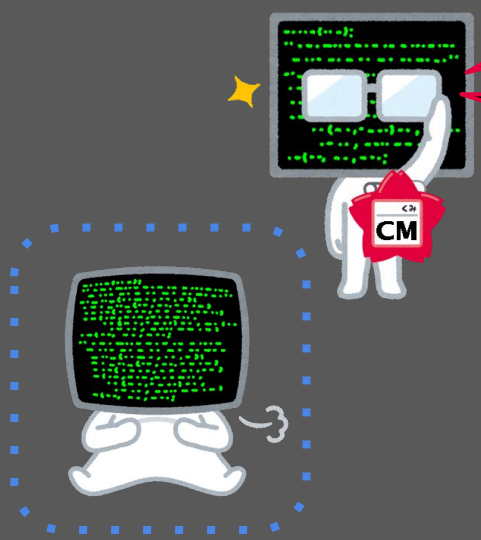

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```



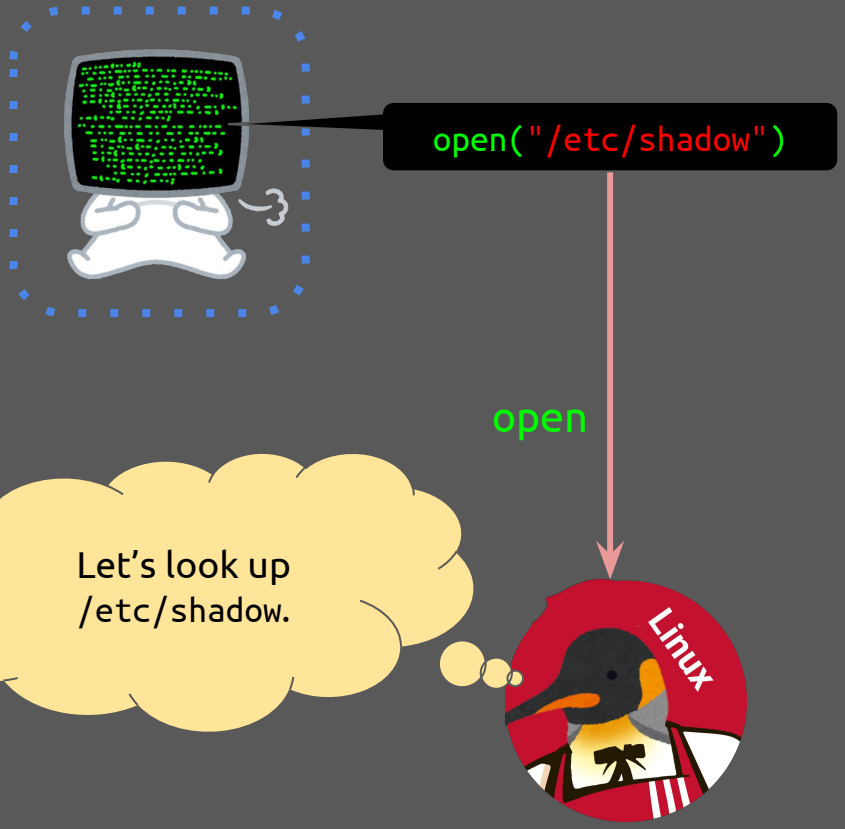

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```




```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```

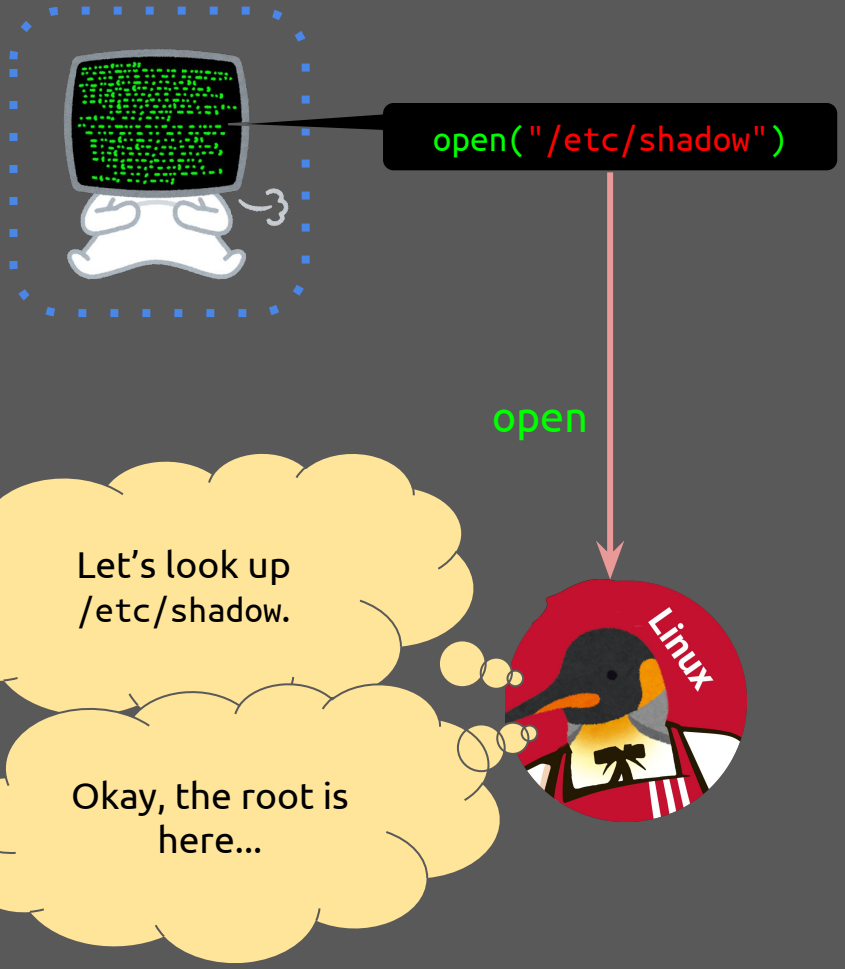



```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            └── files
                └── music.mp3
```



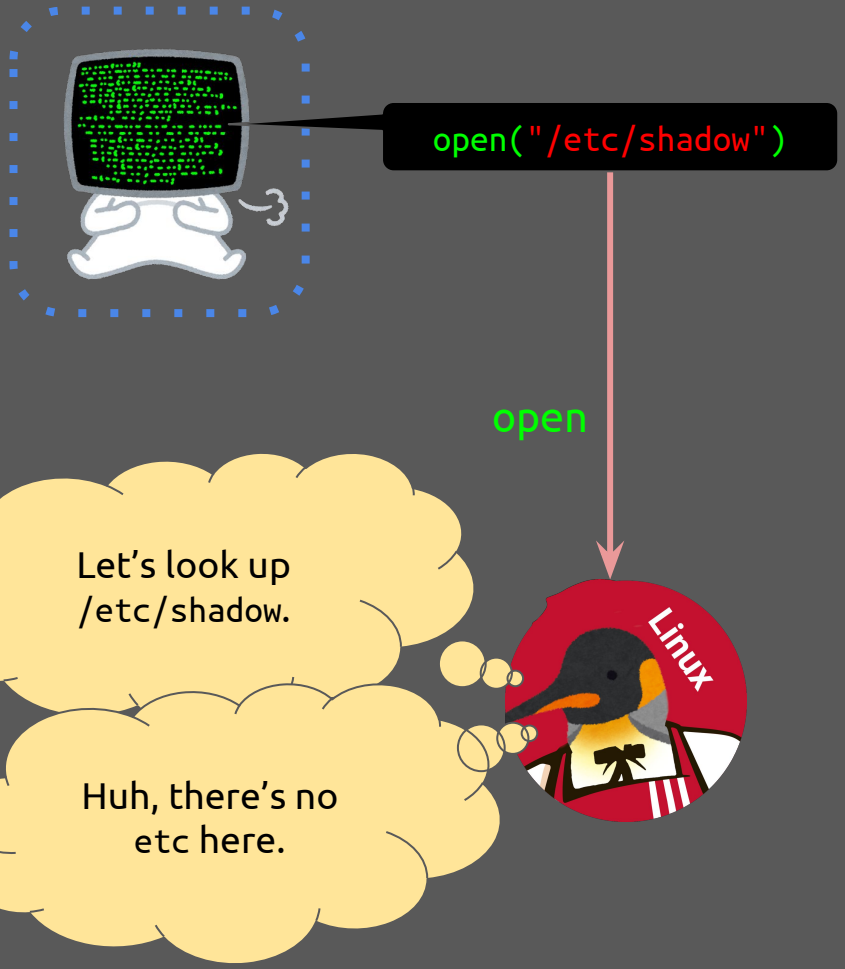
/etc/shadow

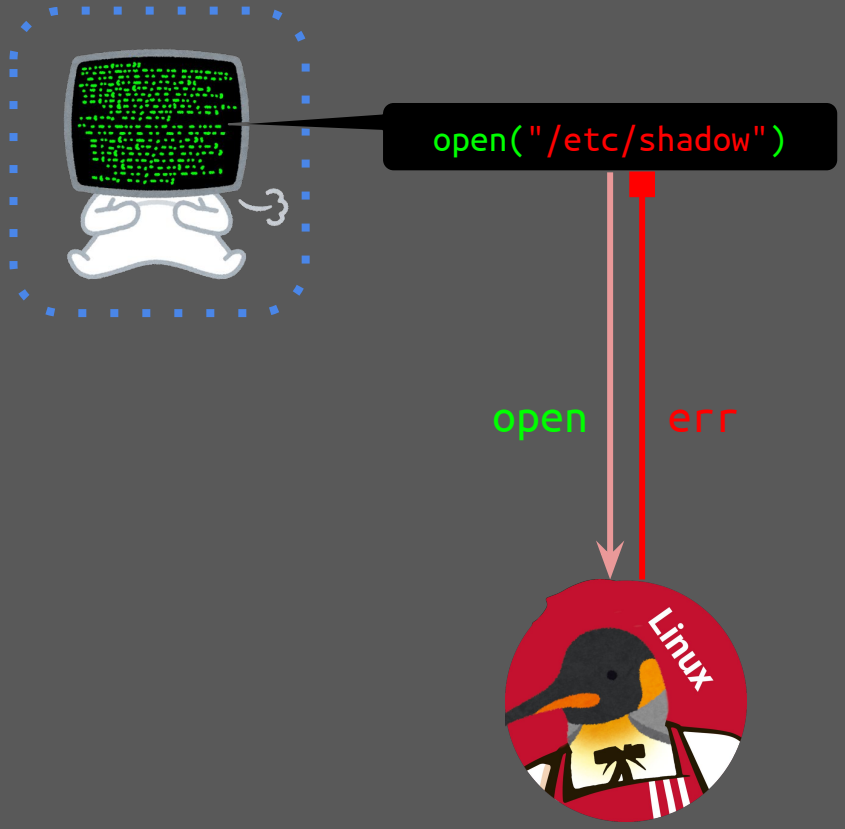
```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```



/etc/shadow

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```


open("/etc/shadow")
open
Let's look up /etc/shadow.
Huh, there's no etc here.
Linux
/etc/shadow
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│   └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3

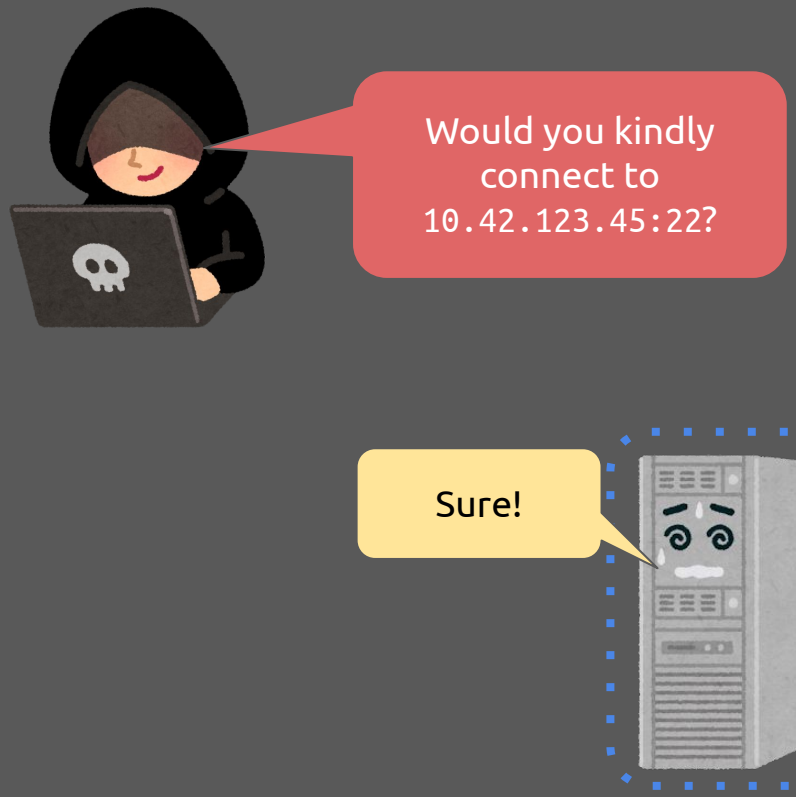


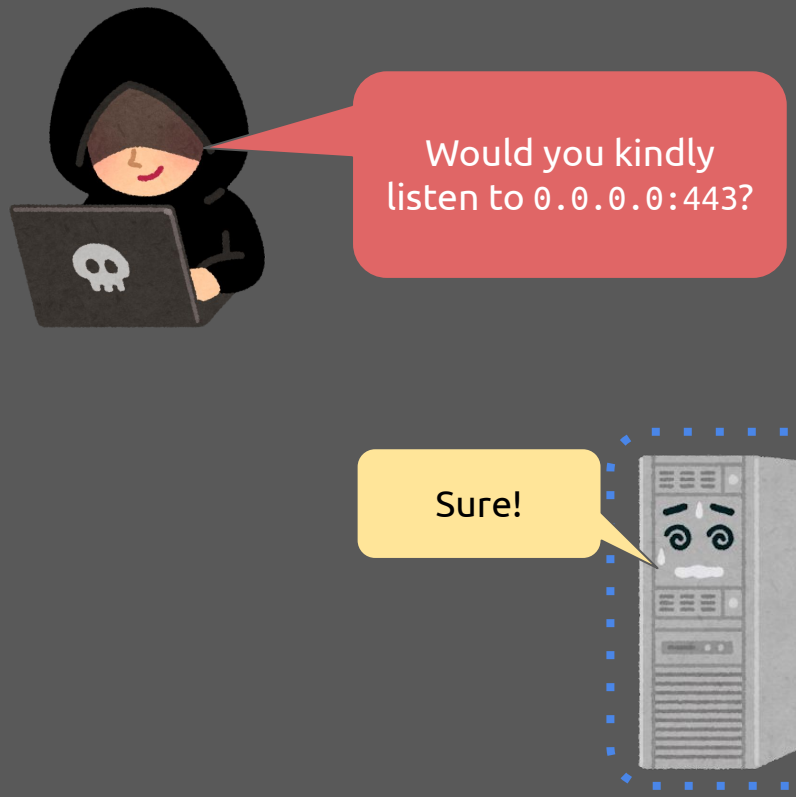

```
/
├── etc
│   └── shadow
├── home
│   └── cyphar
│       └── secrets.txt
└── var
    ├── db
    │   └── userdata
    └── www
        └── htdocs
            ├── index.html
            └── files
                └── music.mp3
```

Container
Manager

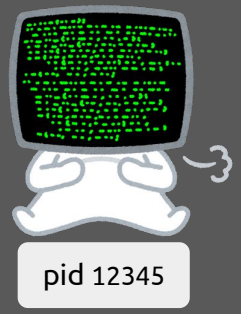
Manager

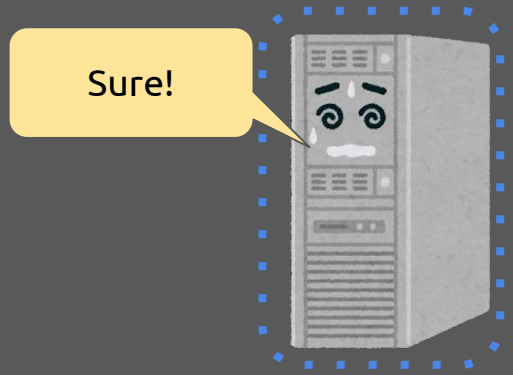

A new foe has app
CM
CHALLENGER APPROACHING

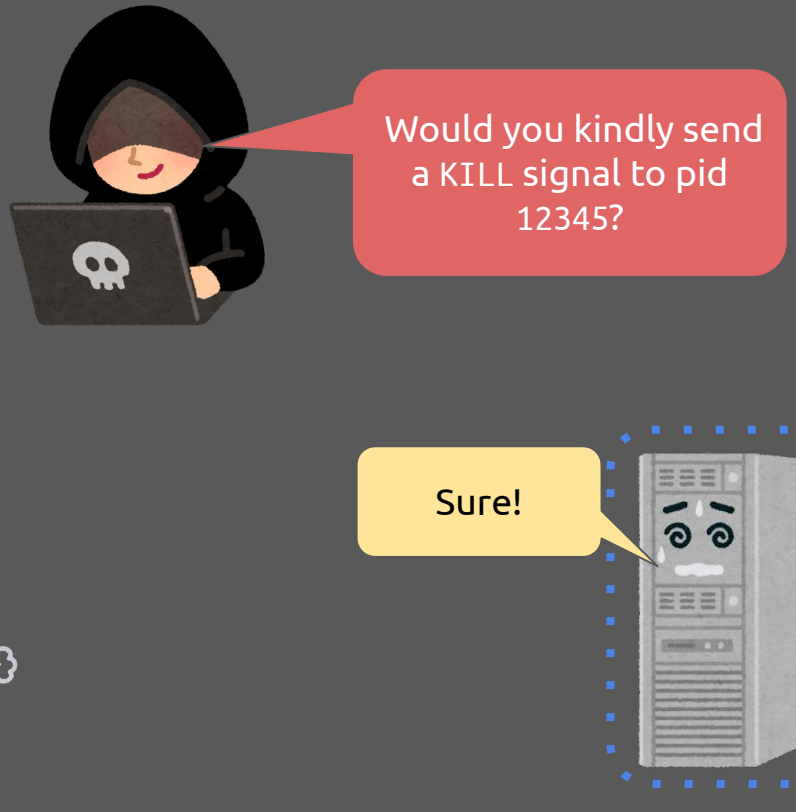

Would you kindly connect to 10.42.123.45:22?
Sure!


Would you kindly listen to 0.0.0.0:443?
Sure!

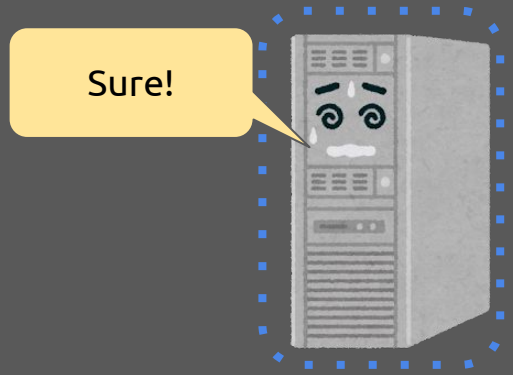

Would you kindly tell me about pid 12345?

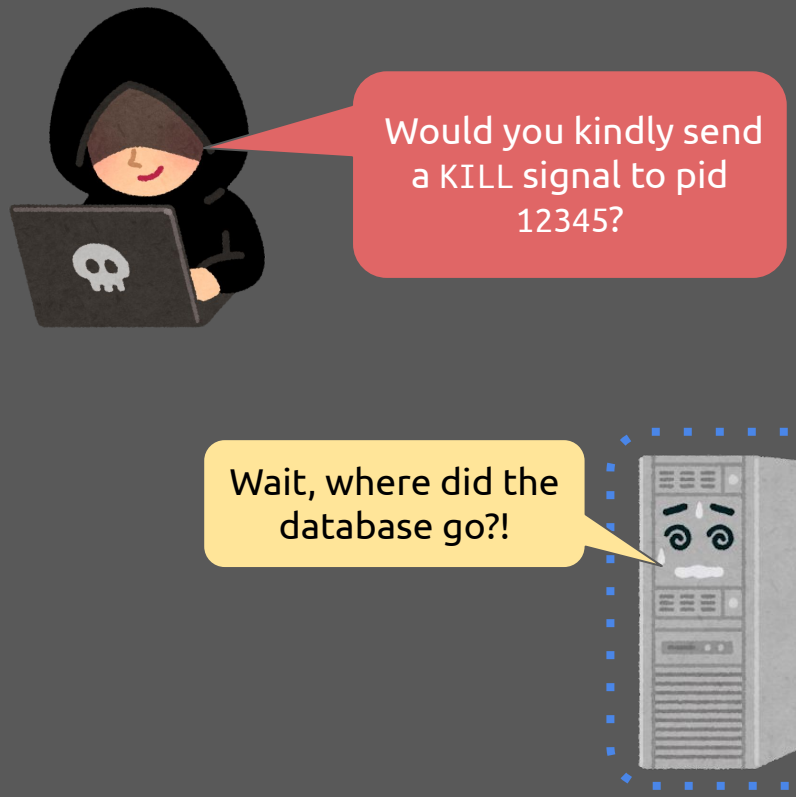

pid 12345


Sure!


Would you kindly send a KILL signal to pid 12345?
Sure!
pid 12345


Would you kindly send a KILL signal to pid 12345?


Sure!

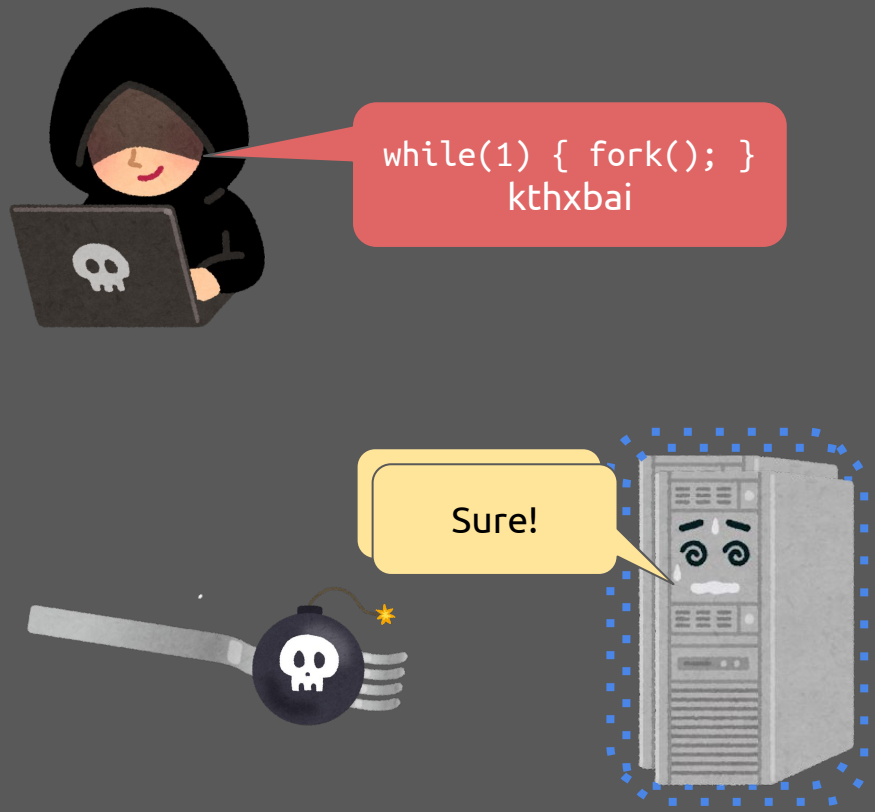

Would you kindly send a KILL signal to pid 12345?
Wait, where did the database go?!

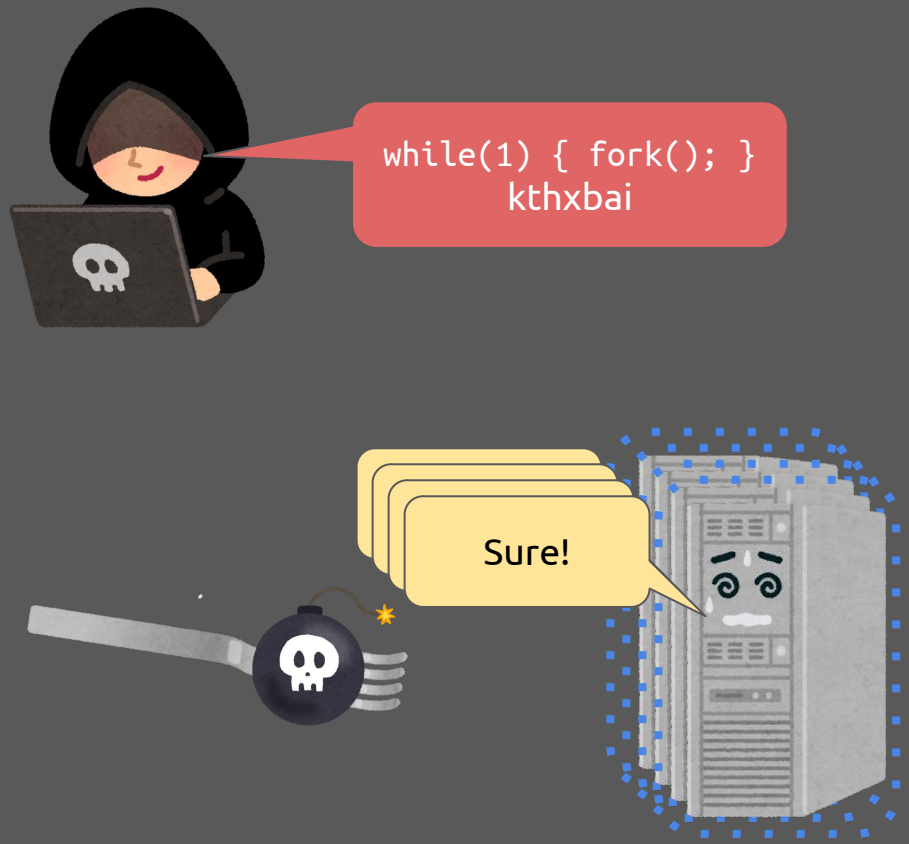

while(1) { fork(); }
kthxbai

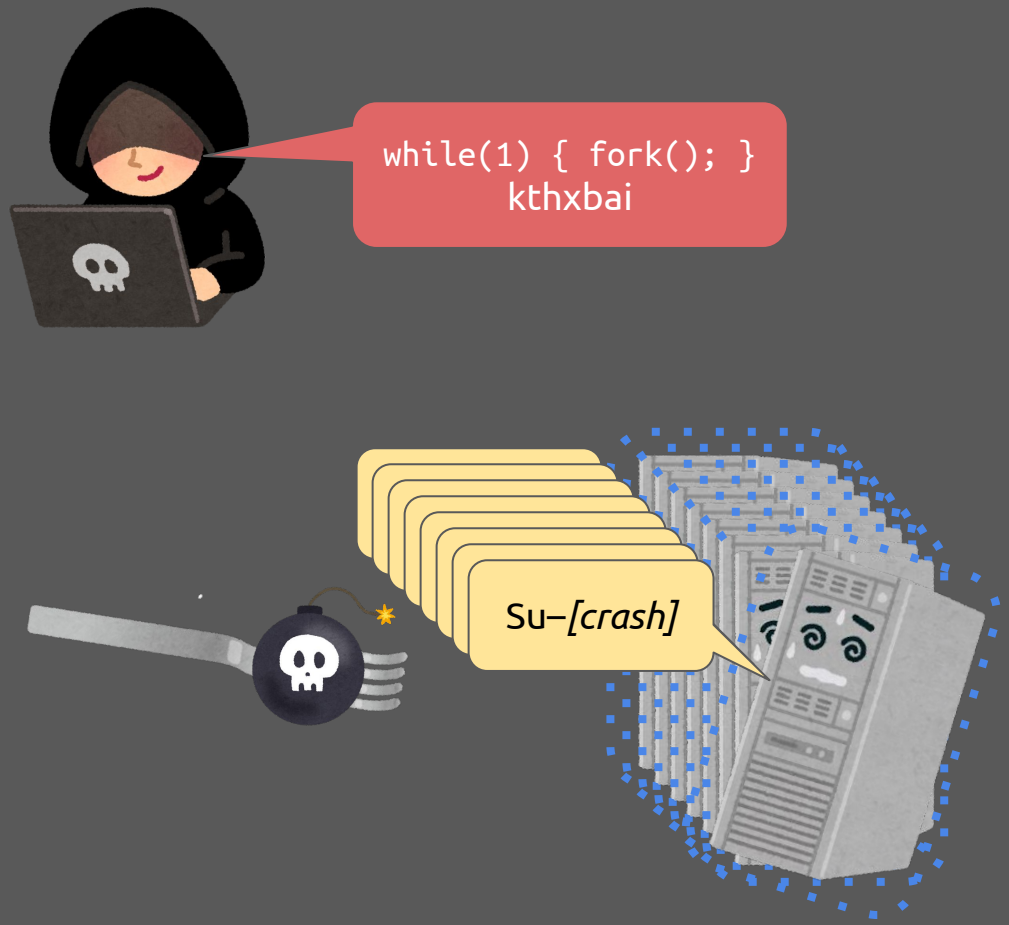

while(1) { fork(); }
kthxbai


while(1) { fork(); }
kthxbai

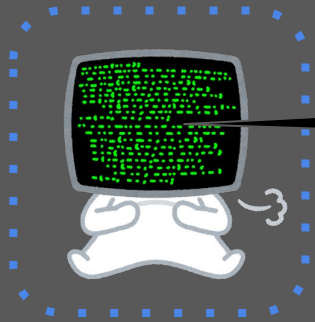

while(1) { fork(); }
kthxbai
Sure!


while(1) { fork(); }
kthxbai
Sure!


while(1) { fork(); }
kthxbai
Sure!


while(1) { fork(); }
kthxbai
Su–[crash]


“just lie even more”

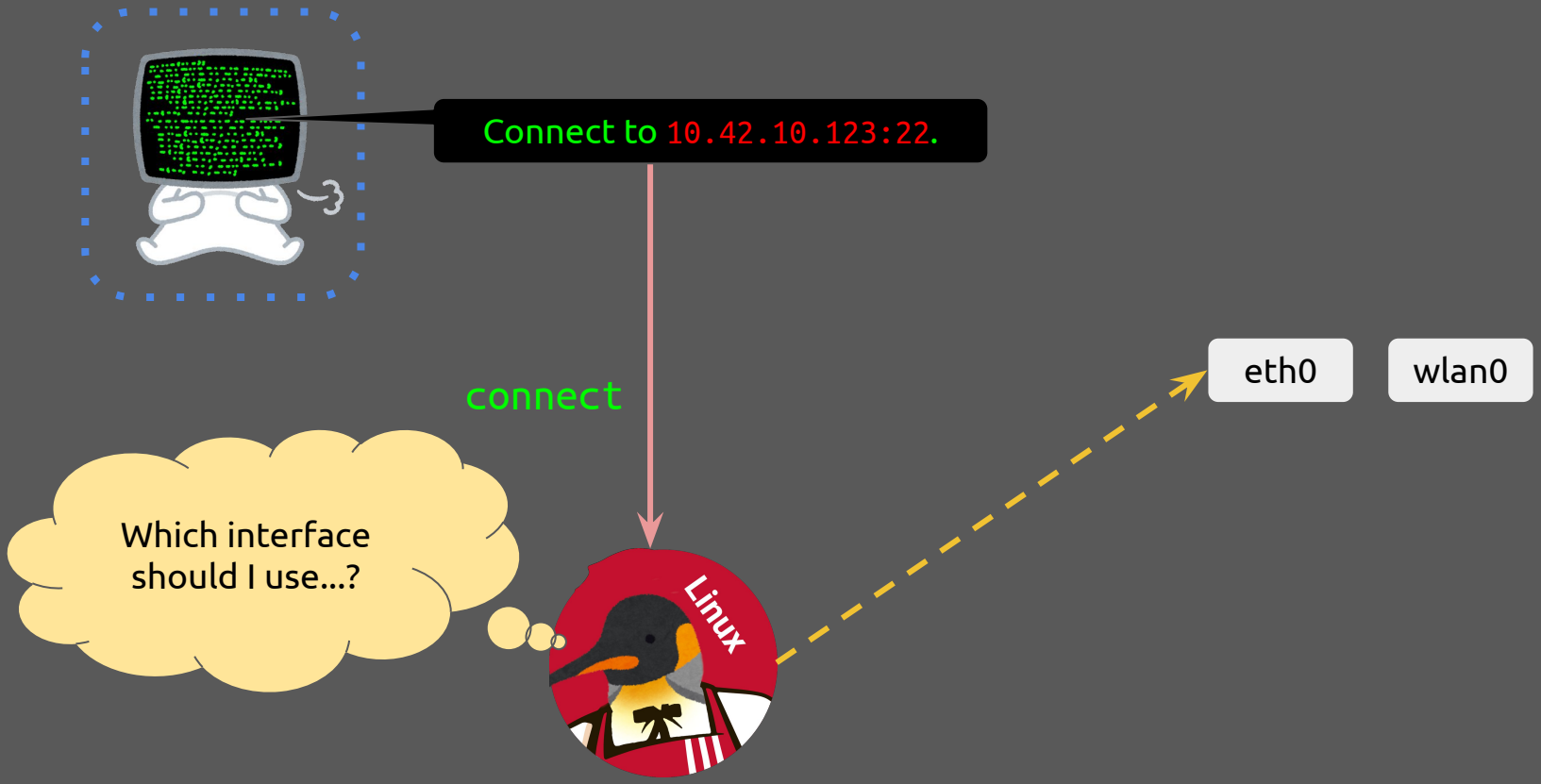


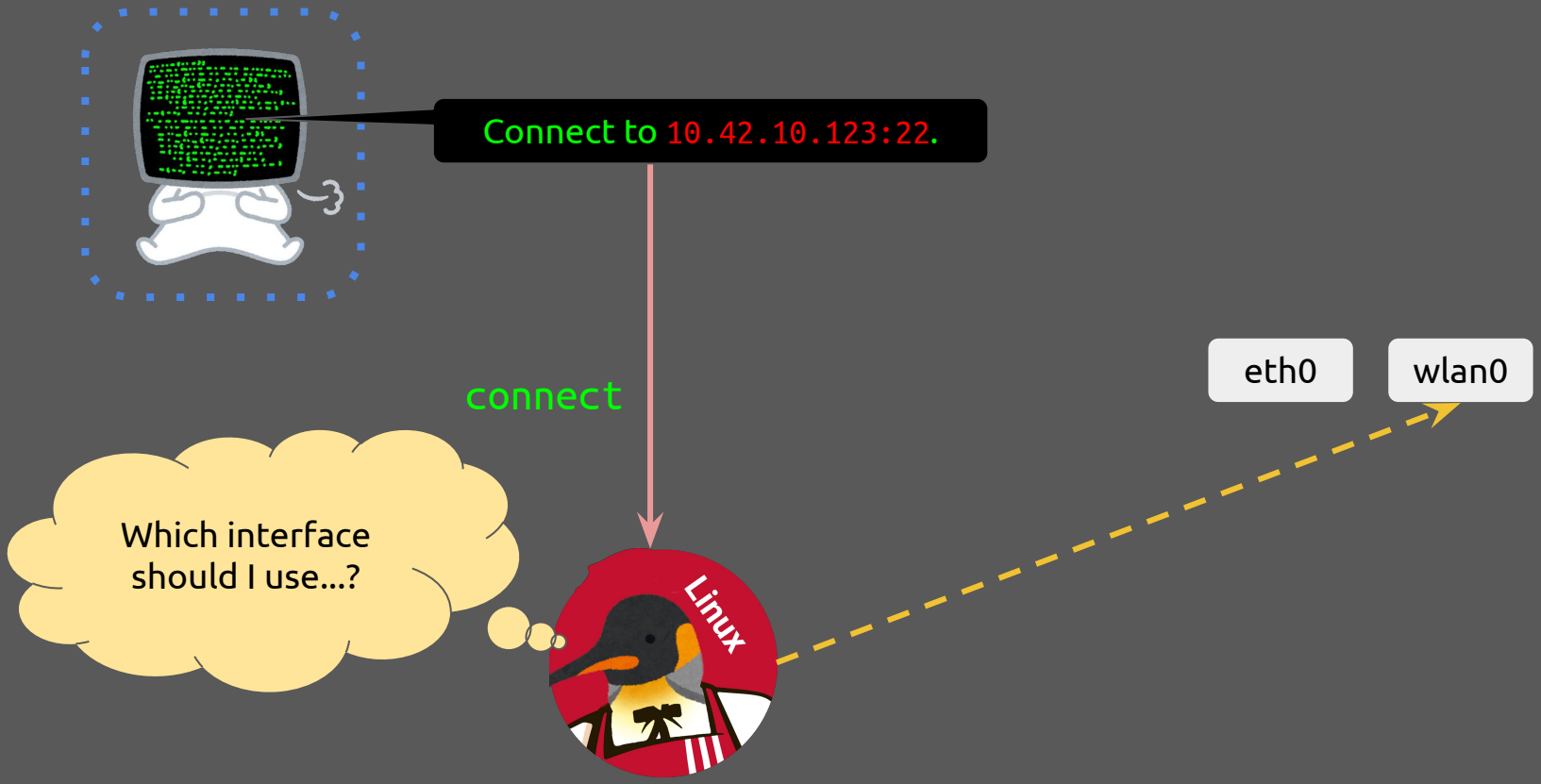
Connect to 10.42.10.123:22.

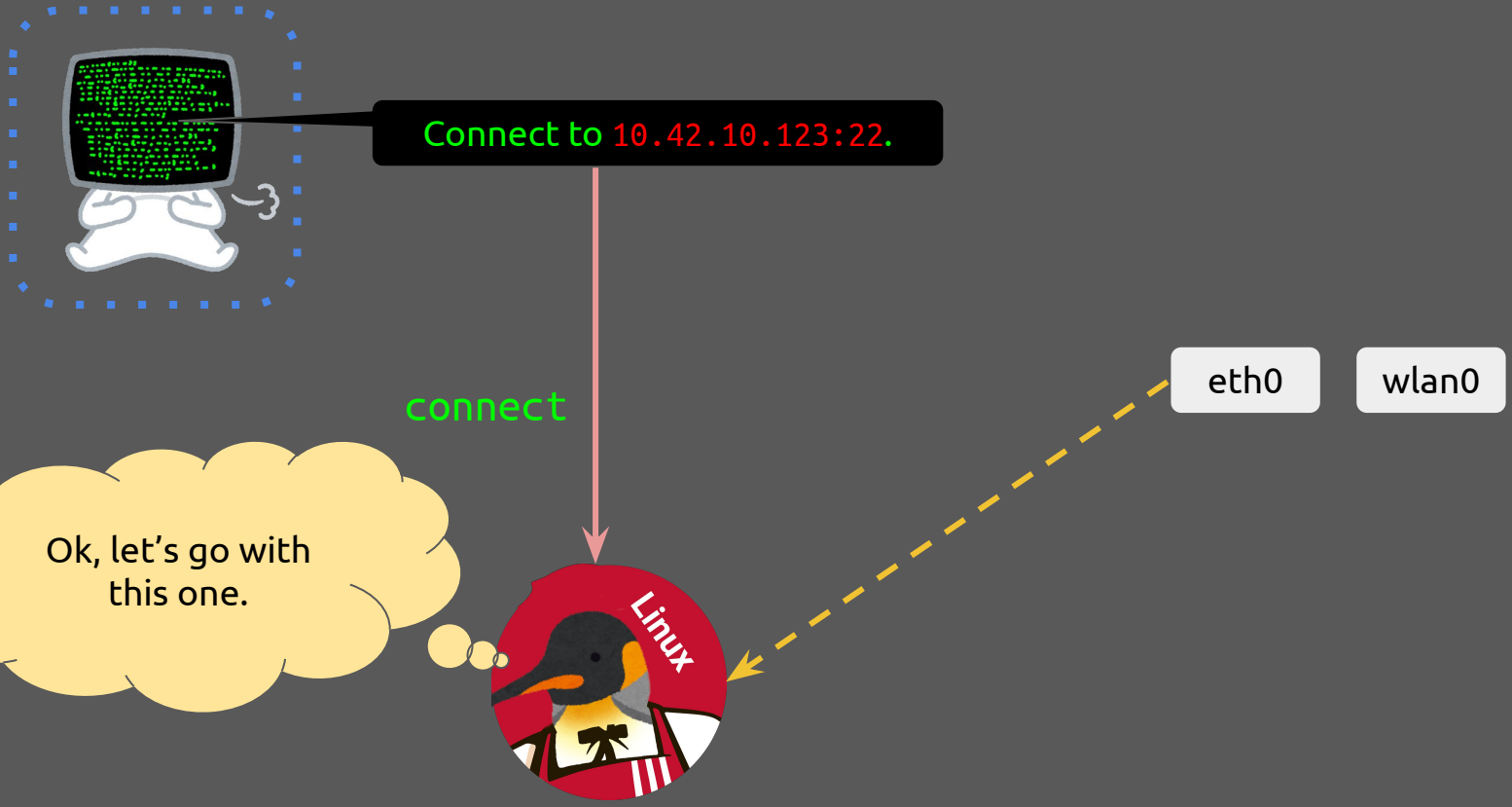
connect

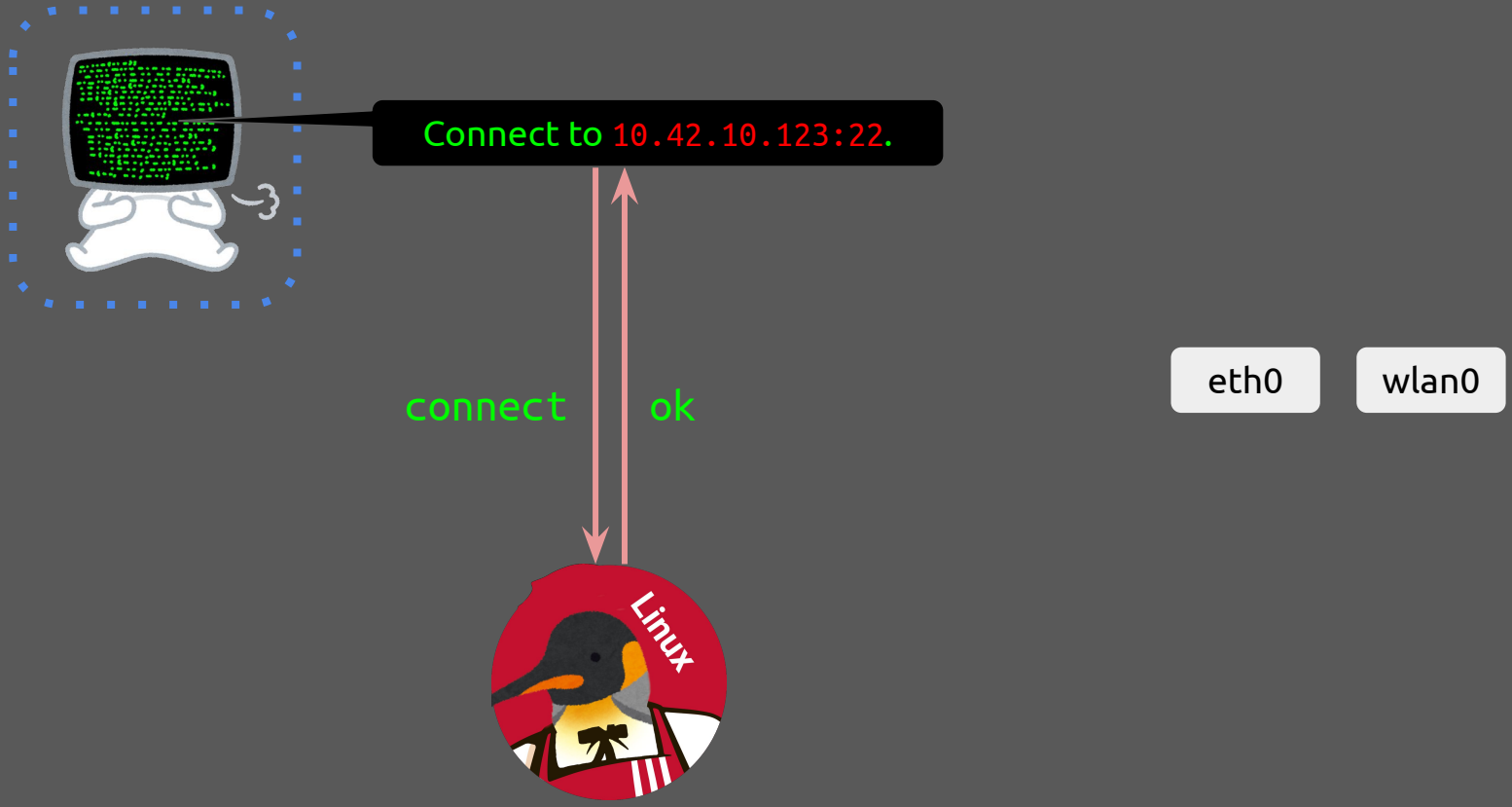
eth0

wlan0


Connect to 10.42.10.123:22.
connect
Which interface
should I use...?
Linux
eth0
wlan0

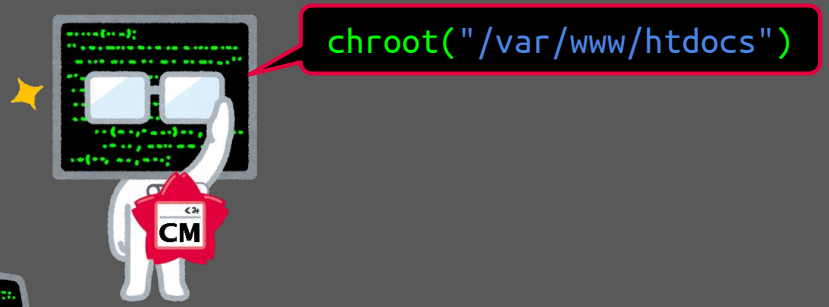

Connect to 10.42.10.123:22.
connect
Which interface
should I use...?
Linux
eth0
wlan0


Connect to 10.42.10.123:22.
connect
eth0
wlan0
Ok, let's go with this one.
Linux


Connect to 10.42.10.123:22.
connect
ok
Linux
eth0
wlan0

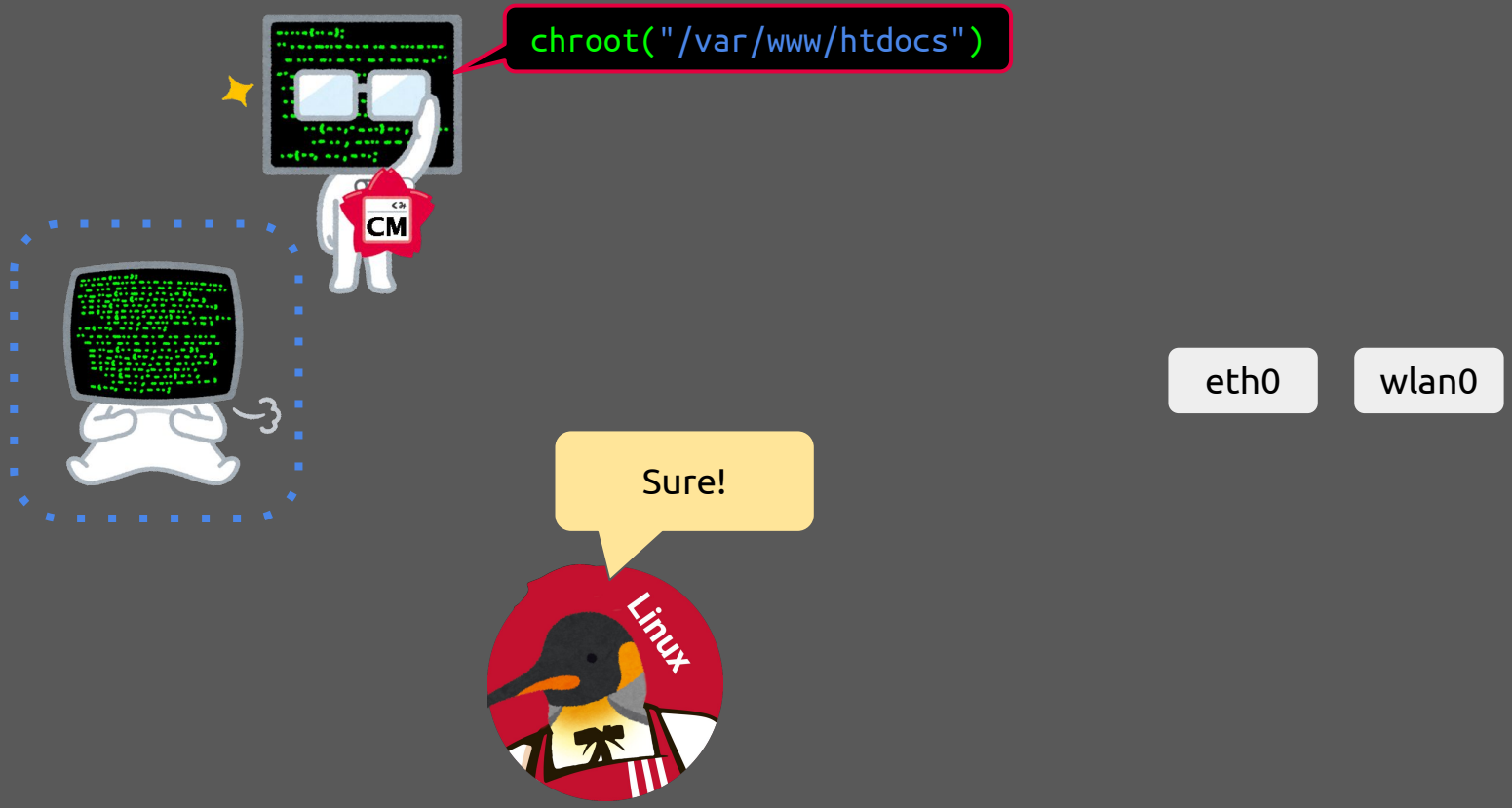
eth0

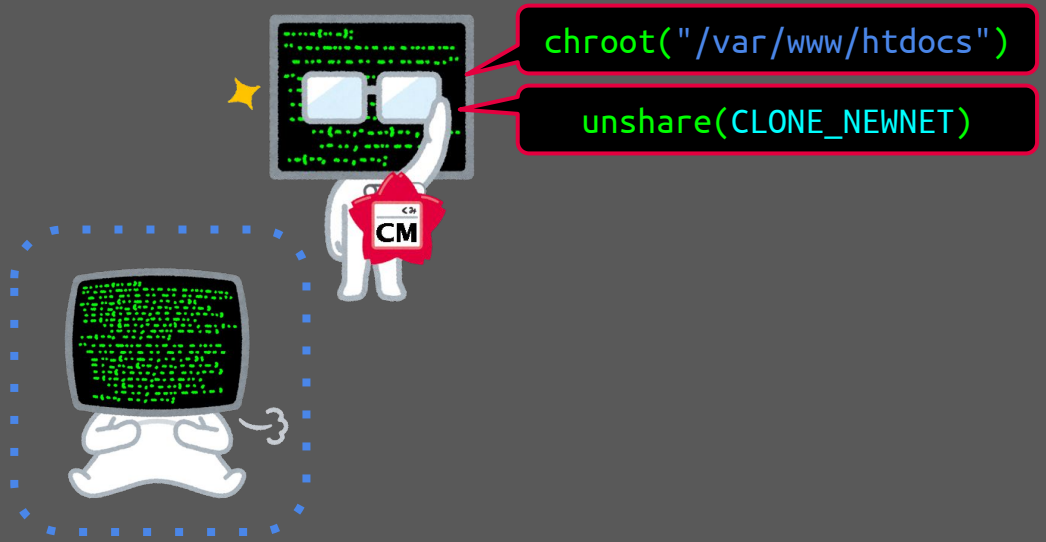
wlan0



eth0

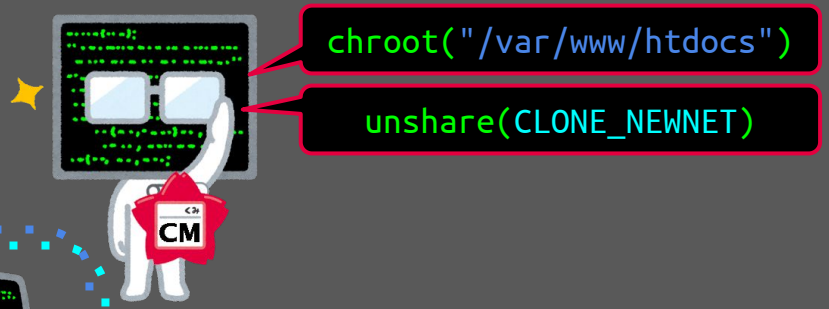
wlan0

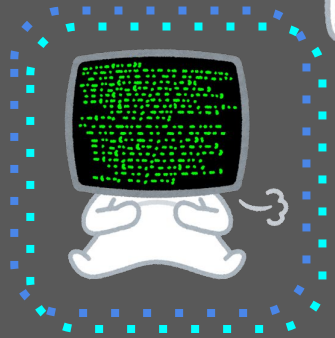

chroot("/var/www/htdocs")
CM
eth0
wlan0
Sure!
Linux



eth0

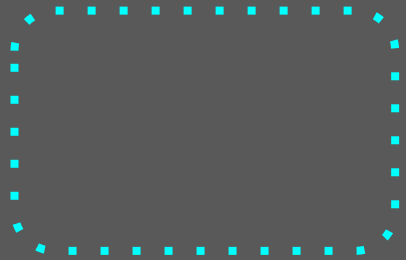
wlan0

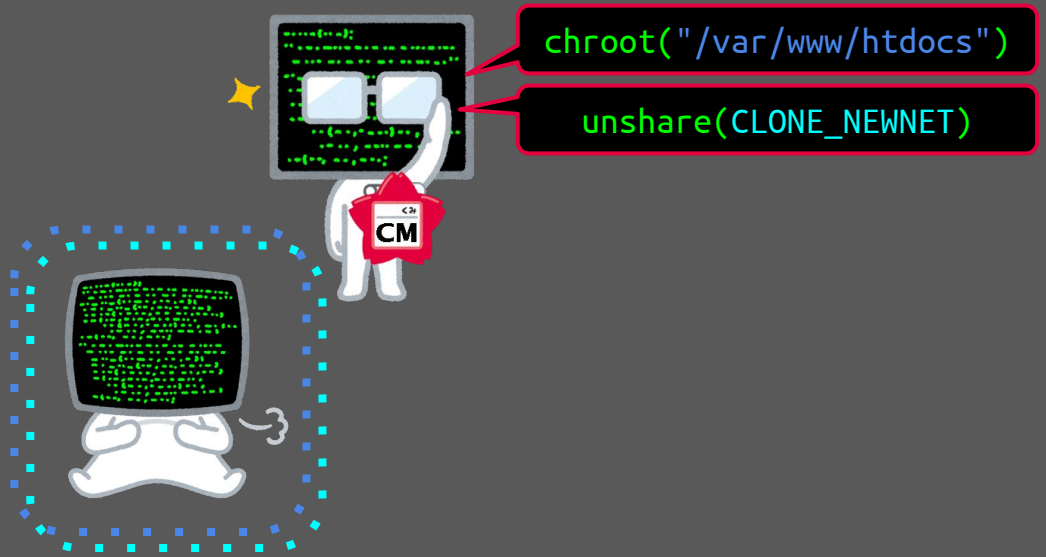




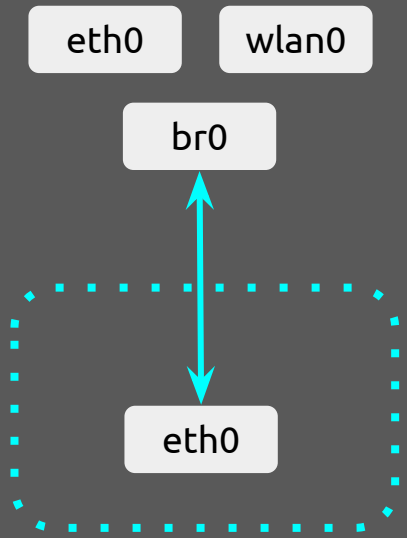
Sure!

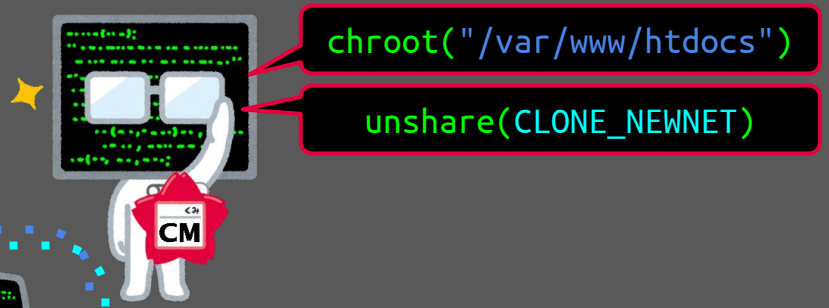
eth0 wlan0

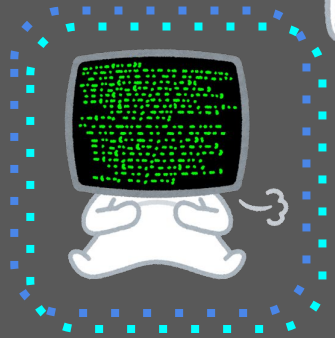



chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
CM

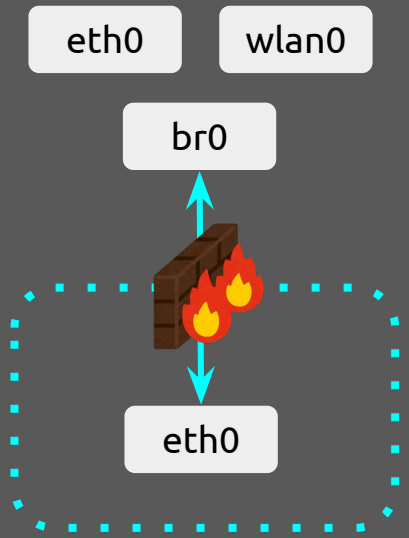

Linux

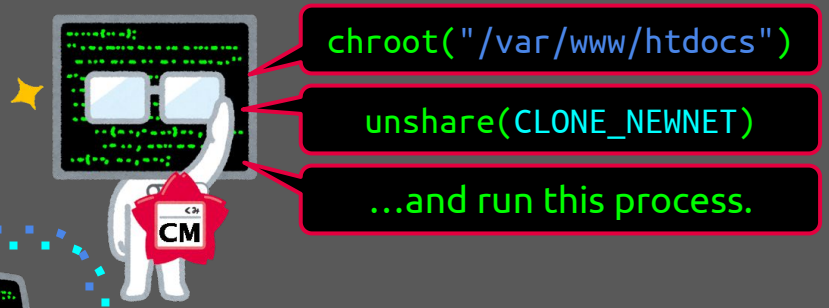

eth0
wlan0
br0
eth0

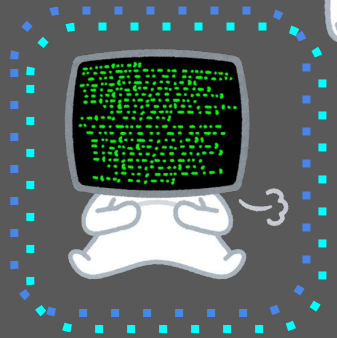

chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
CM



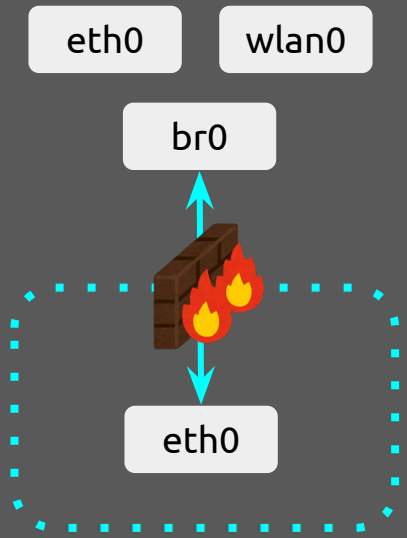

Linux

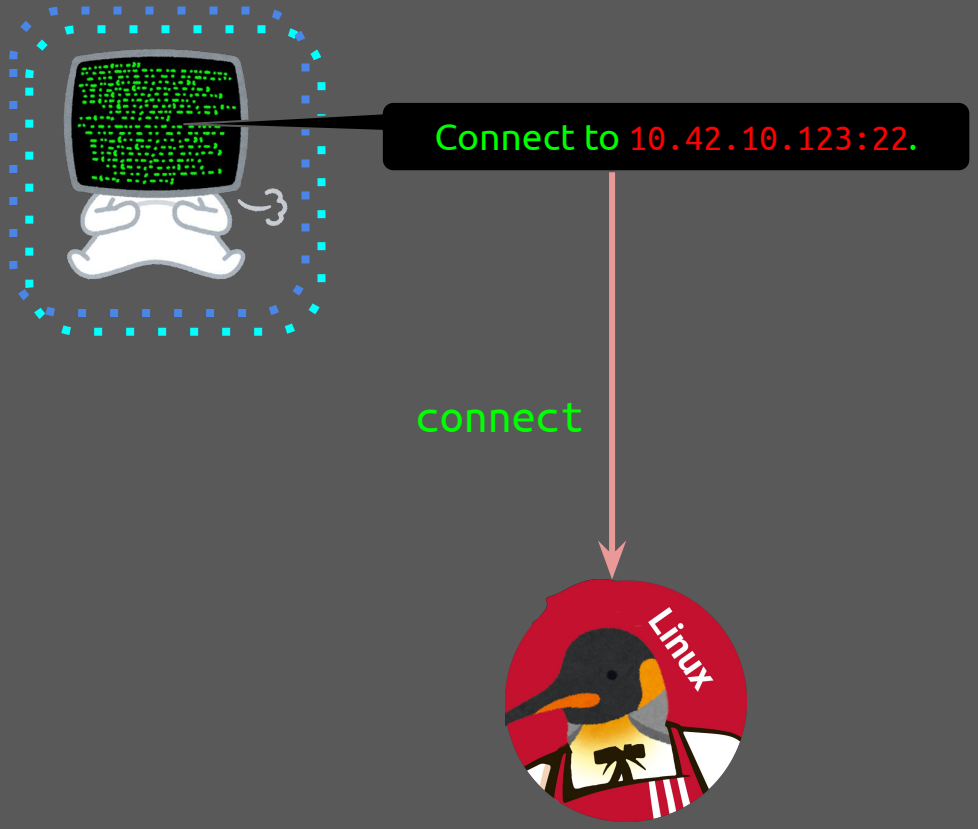

eth0
wlan0
br0
eth0

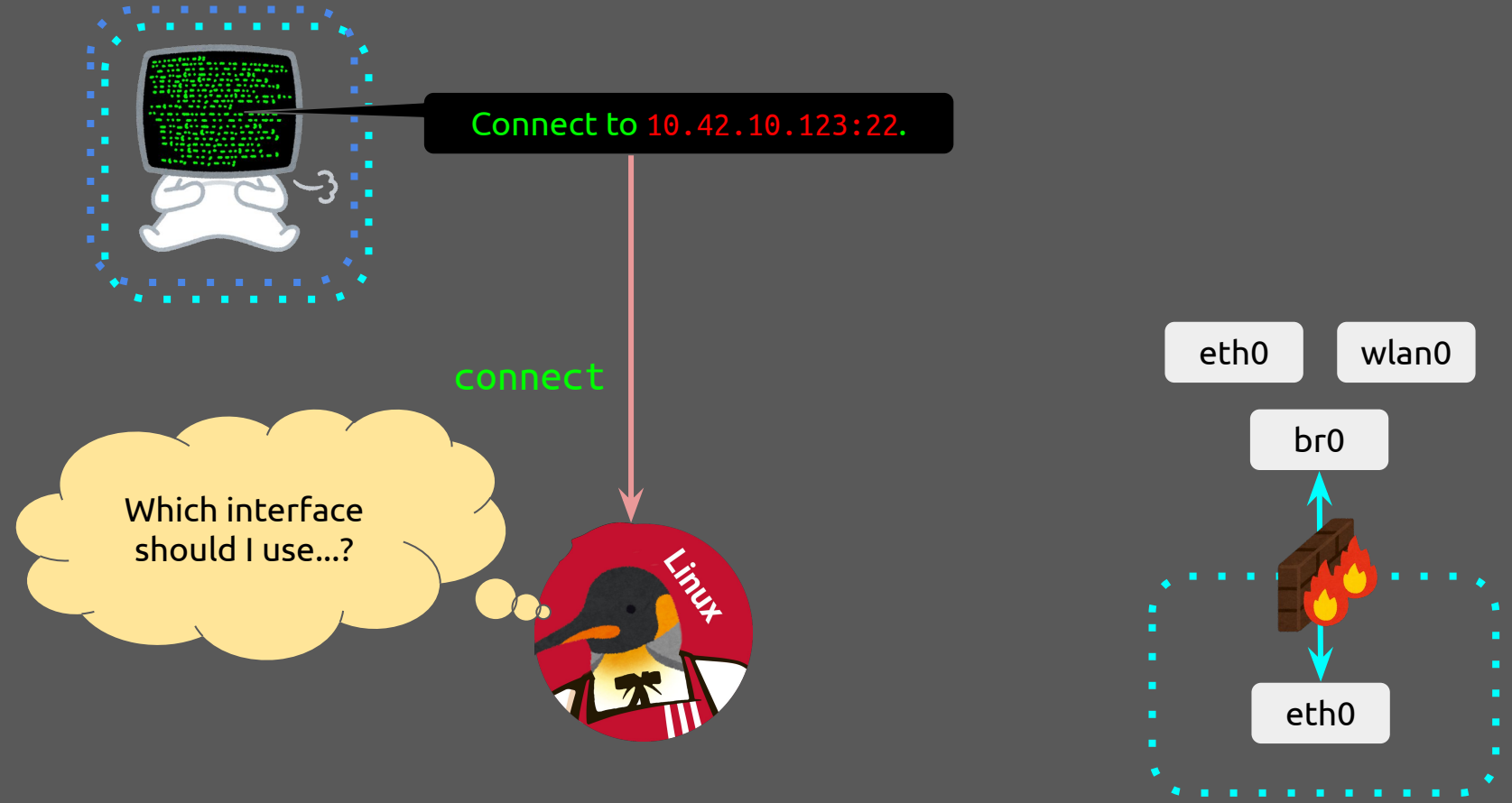

chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
...and run this process.
CM

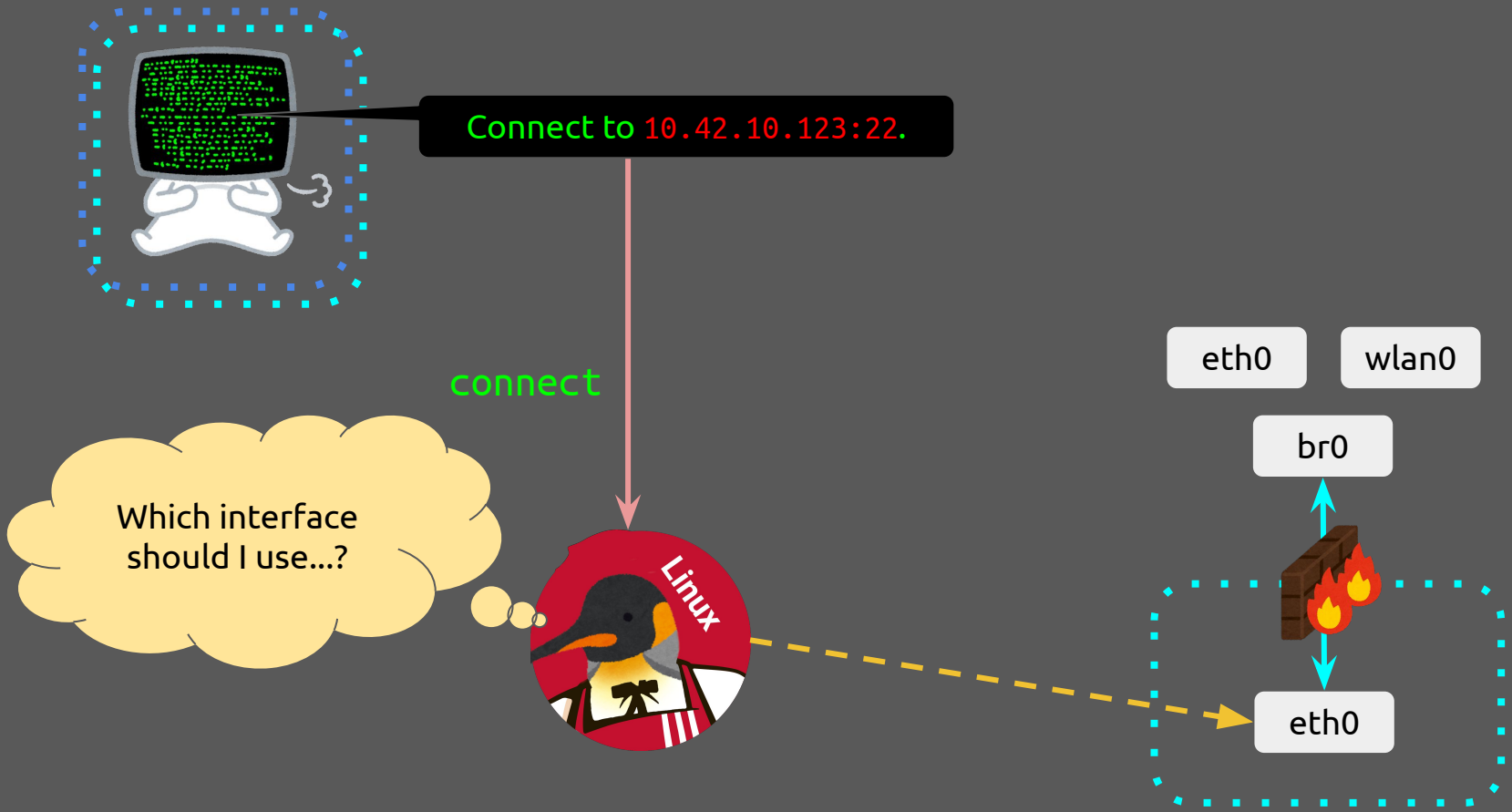


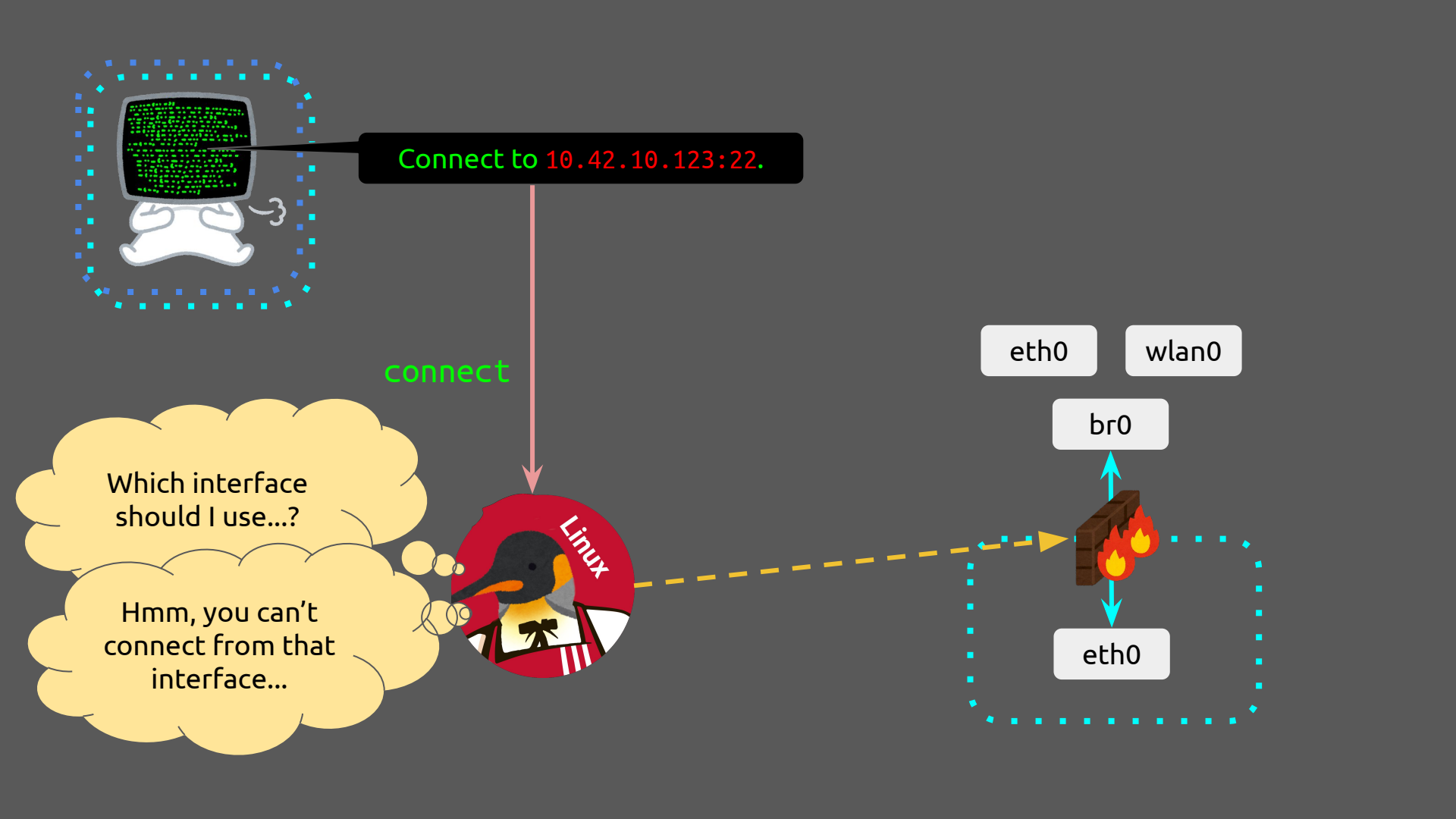

Linux

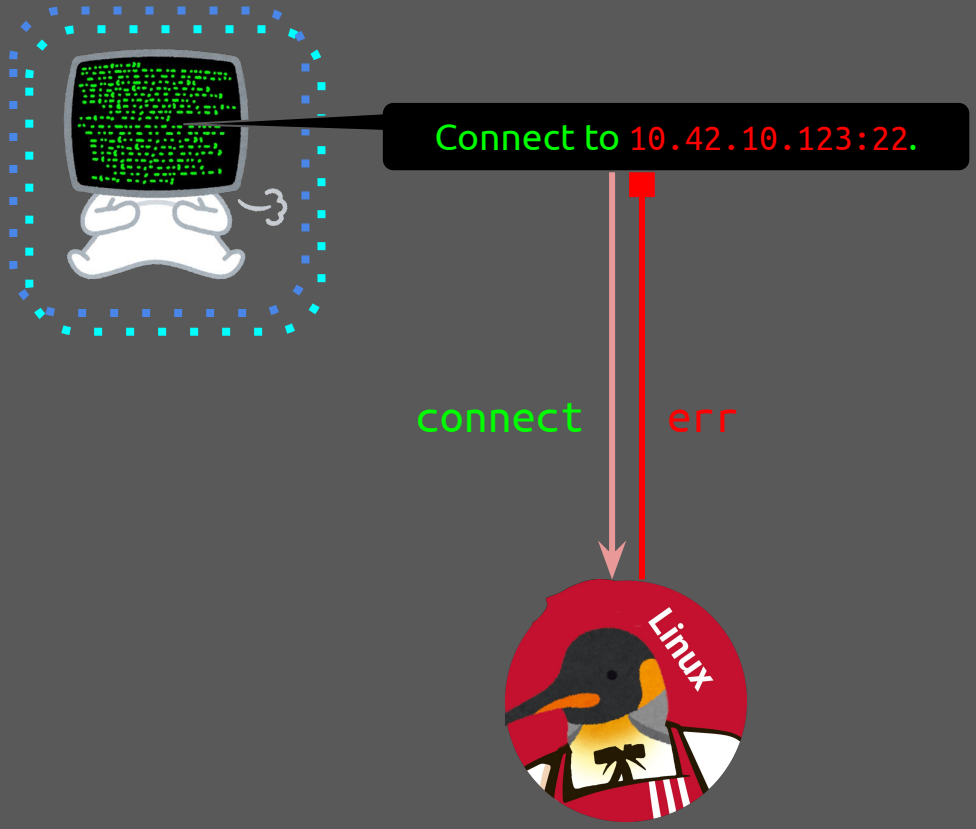

eth0
wlan0
br0
eth0

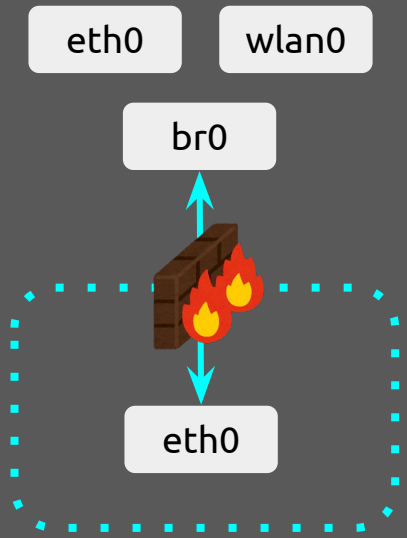

Connect to 10.42.10.123:22.
connect
Linux
eth0
wlan0
br0
eth0

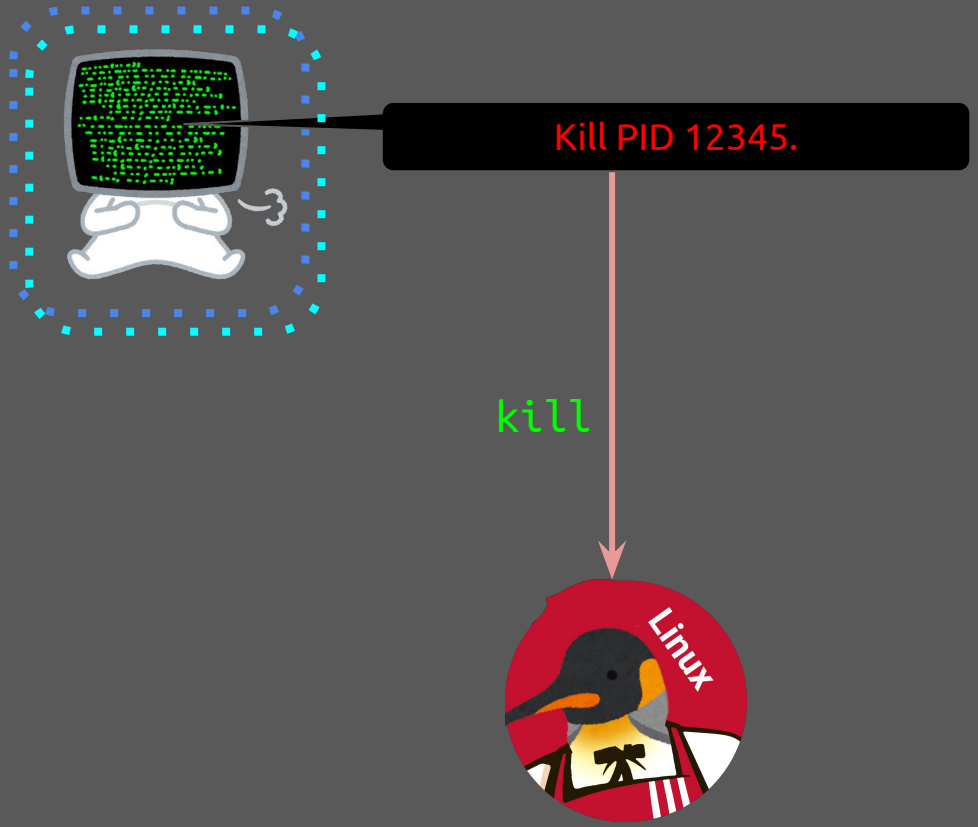

Connect to 10.42.10.123:22.
connect
Which interface
should I use...?
Linux
eth0
wlan0
br0
eth0

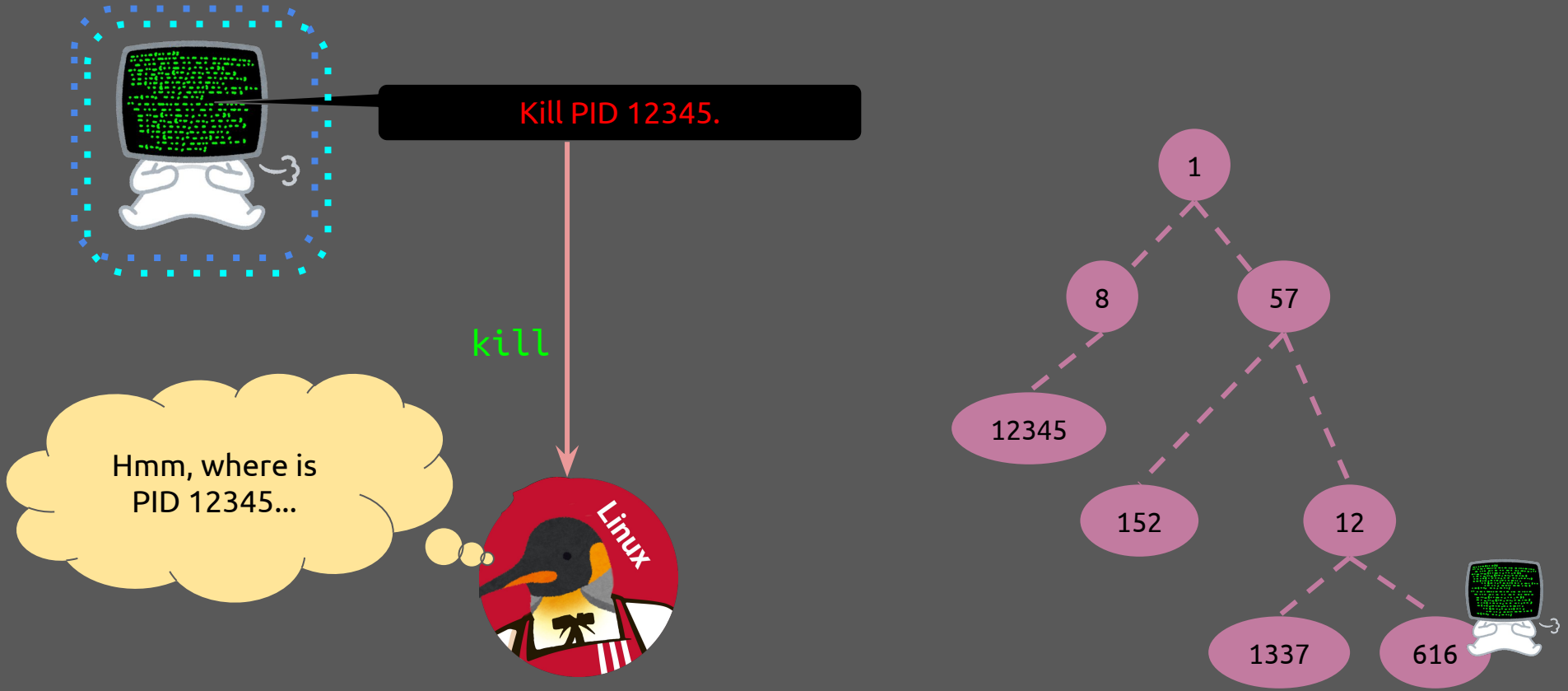

Connect to 10.42.10.123:22.
connect
Which interface
should I use...?
Linux
eth0
wlan0
br0
eth0

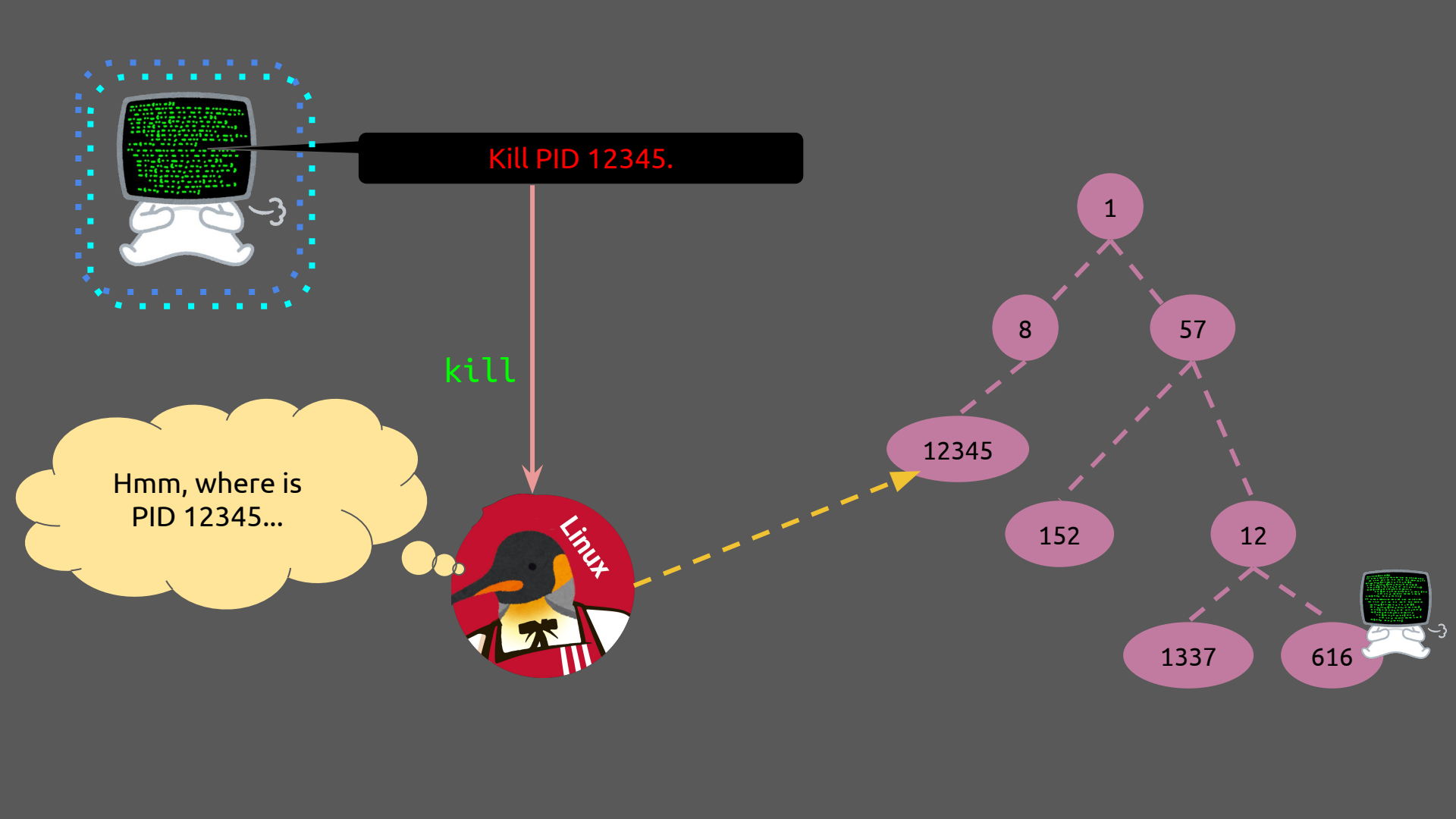

Connect to 10.42.10.123:22.
connect
Which interface should I use...?
Hmm, you can't connect from that interface...
Linux
eth0
wlan0
br0
eth0

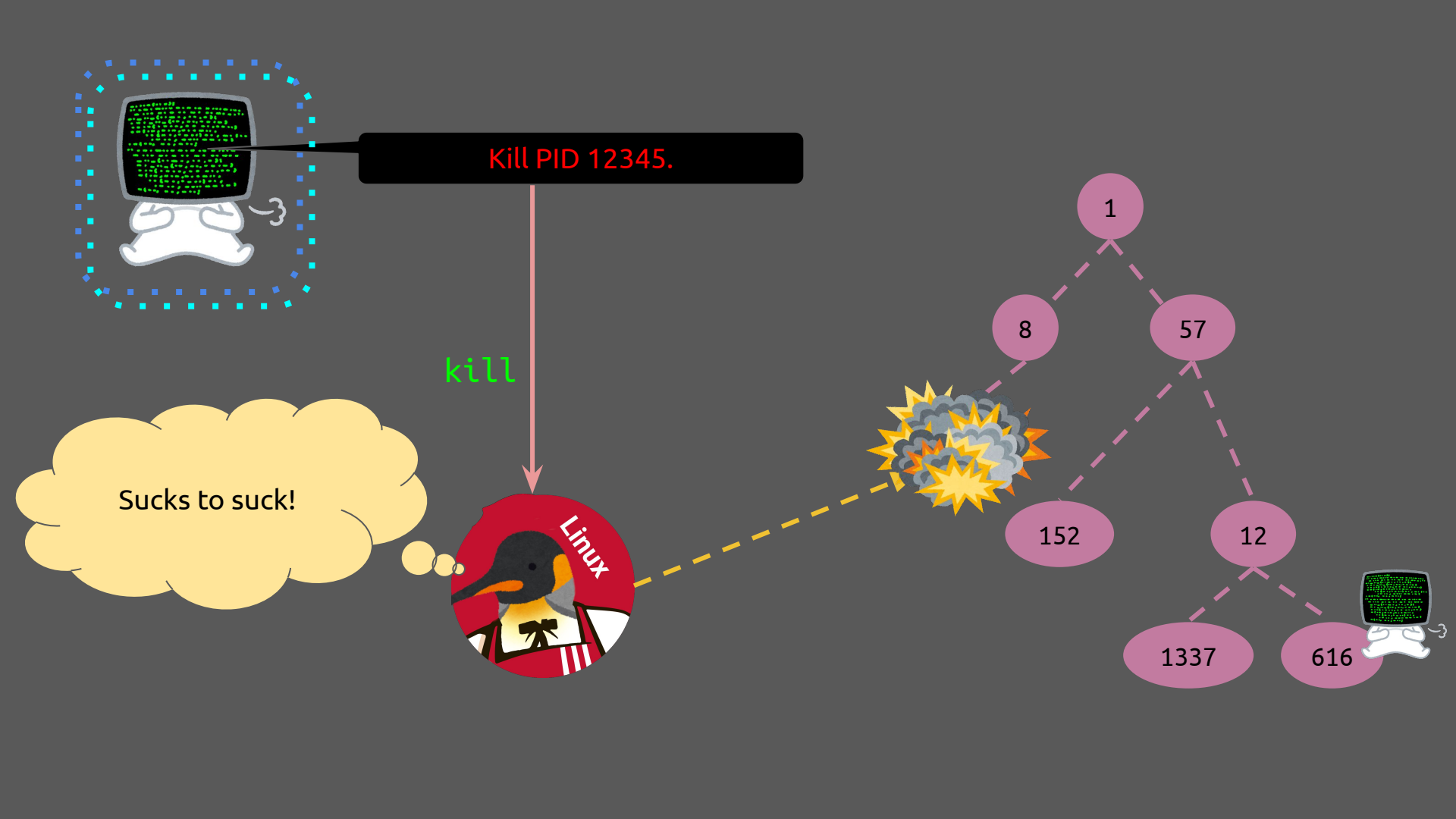

Connect to 10.42.10.123:22.
connect
err
Linux

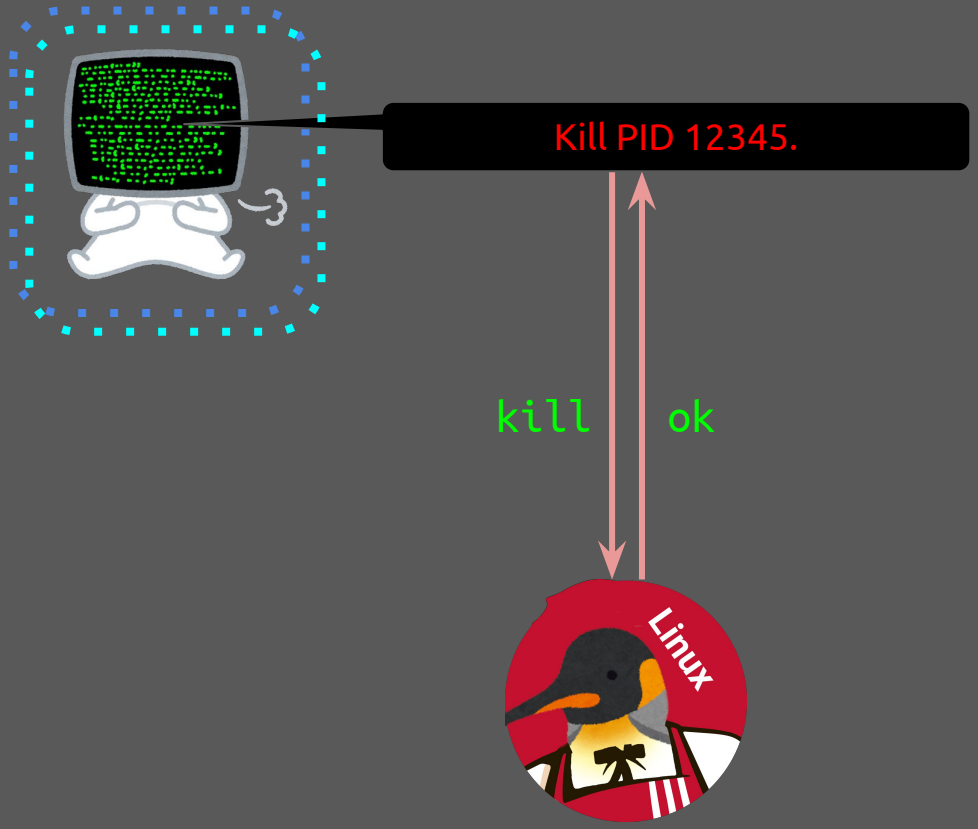

eth0
wlan0
br0
eth0

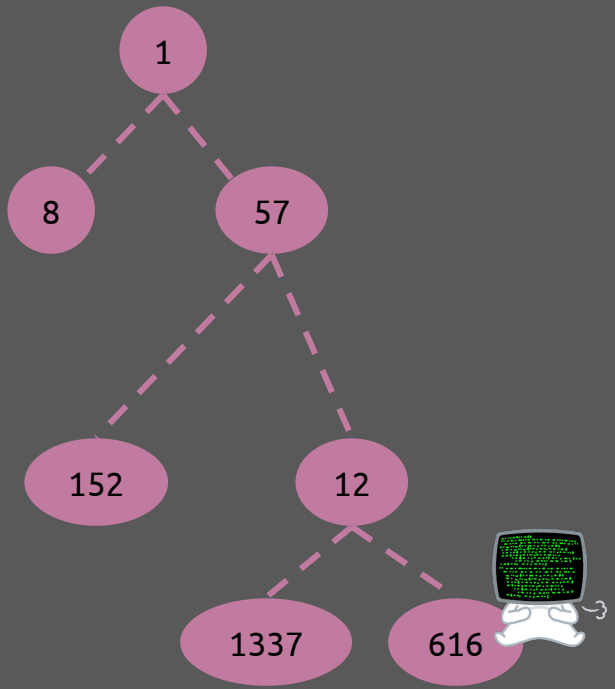

Kill PID 12345.
kill
Linux
1
8
57
12345
152
12
1337
616


Kill PID 12345.
kill
Hmm, where is
PID 12345...
Linux
1
8
57
12345
152
12
1337
616


Kill PID 12345.
kill
Hmm, where is
PID 12345...
Linux
1
8
57
12345
152
12
1337
616

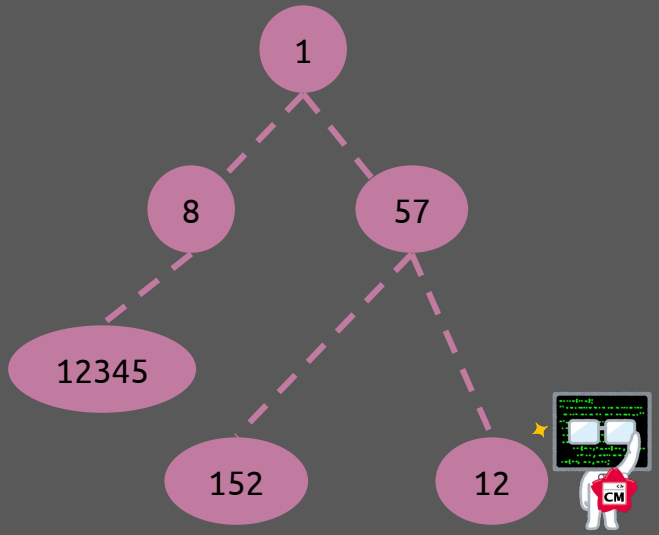

Kill PID 12345.
kill
Sucks to suck!
Linux
1
8
57
152
12
1337
616

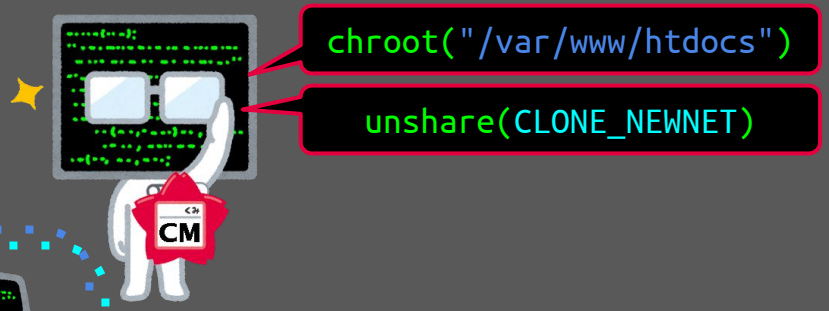

Kill PID 12345.
kill
ok
Linux

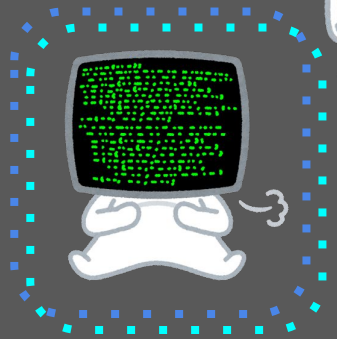

1
8
57
152
12
1337
616


CM

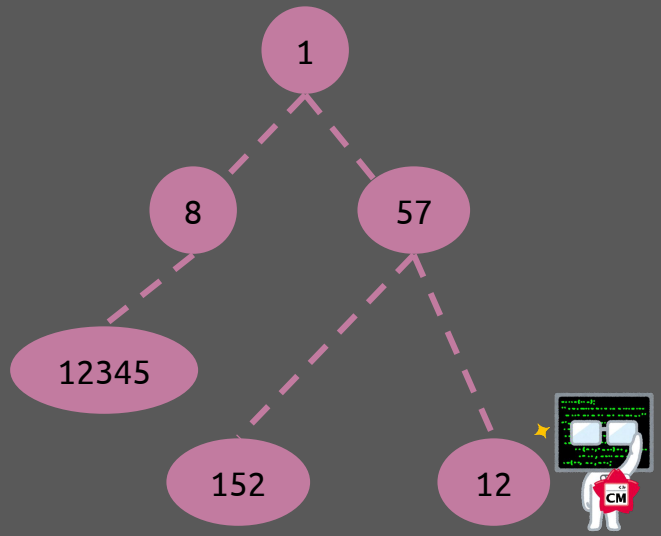

Linux

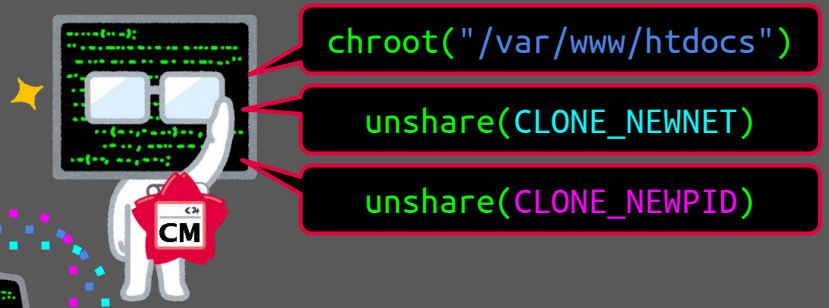

1
8
57
12345
152
12
CM

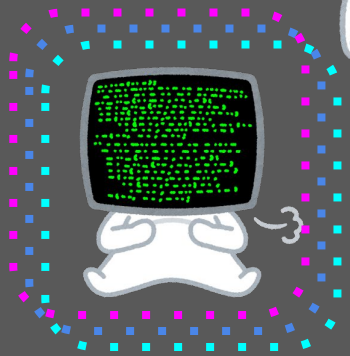

chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
CM



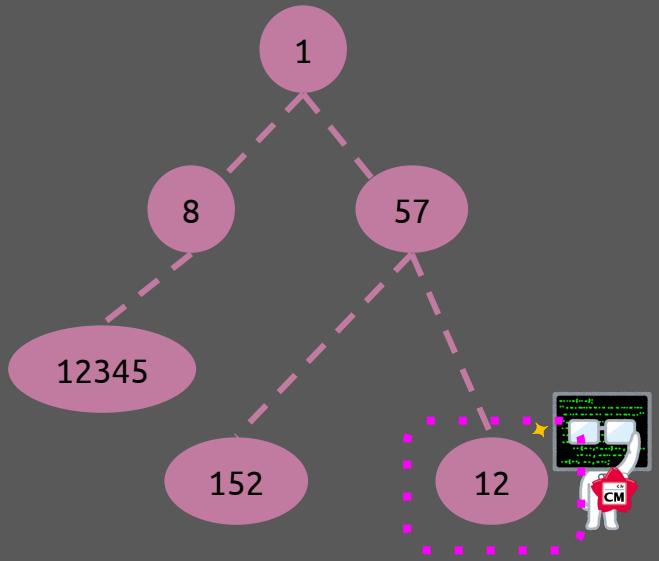

Sure!
Linux

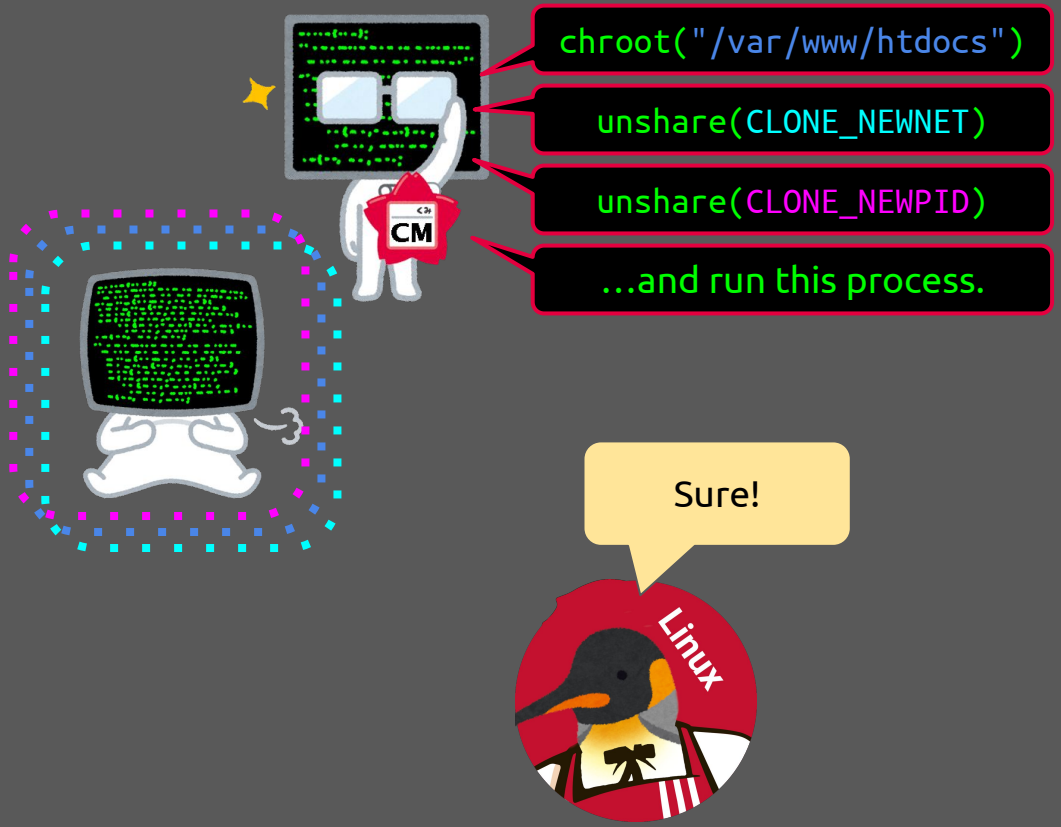

1
8
57
12345
152
12
CM

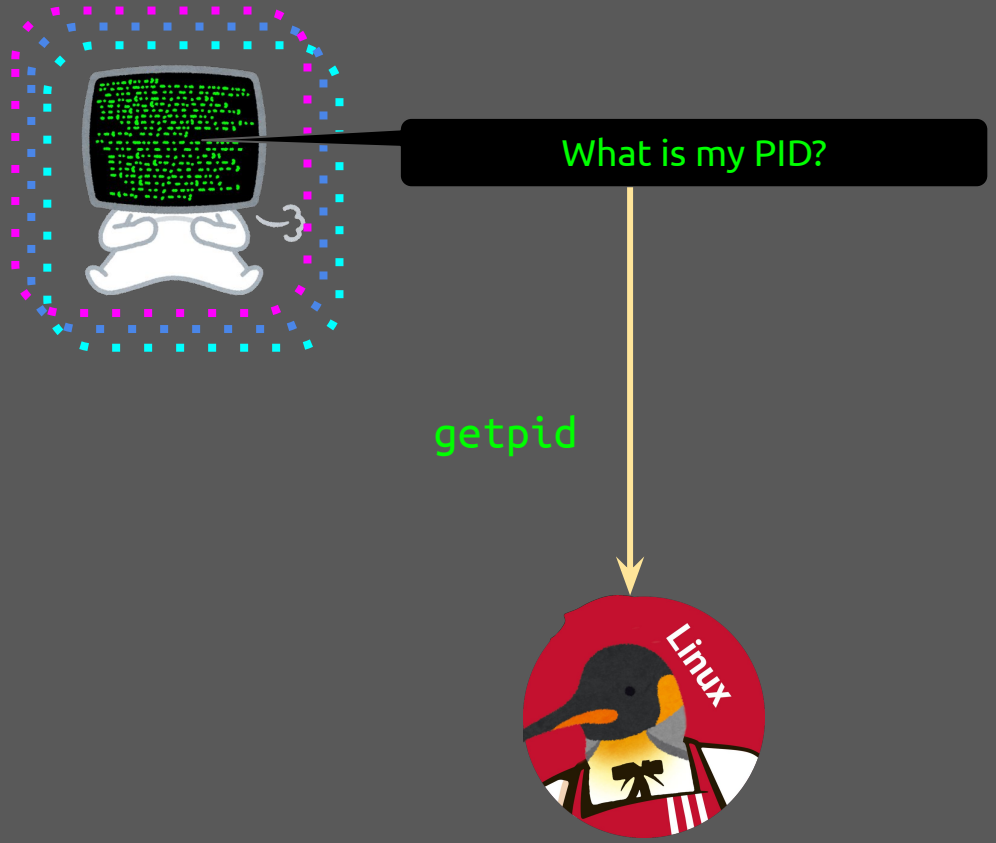

chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
unshare(CLONE_NEWPID)
CM

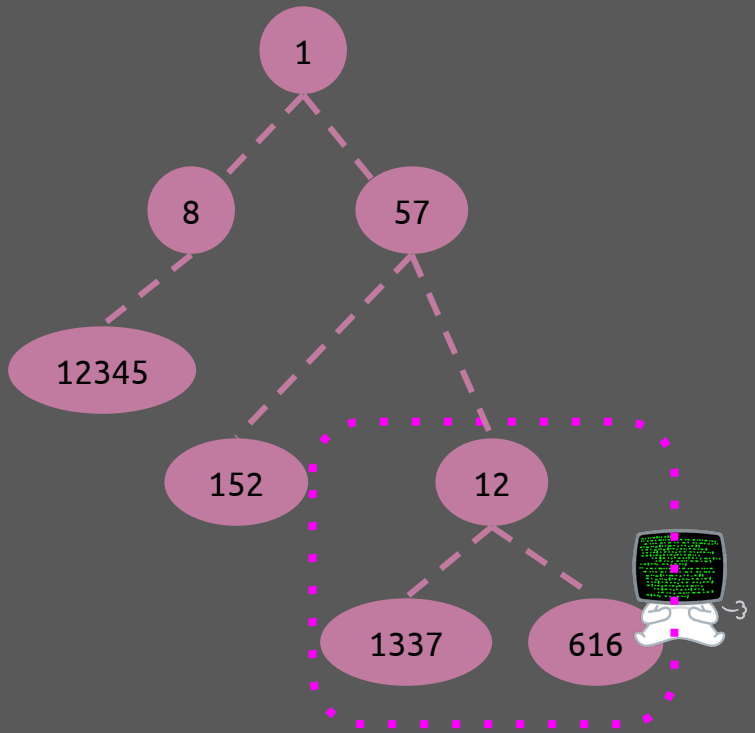


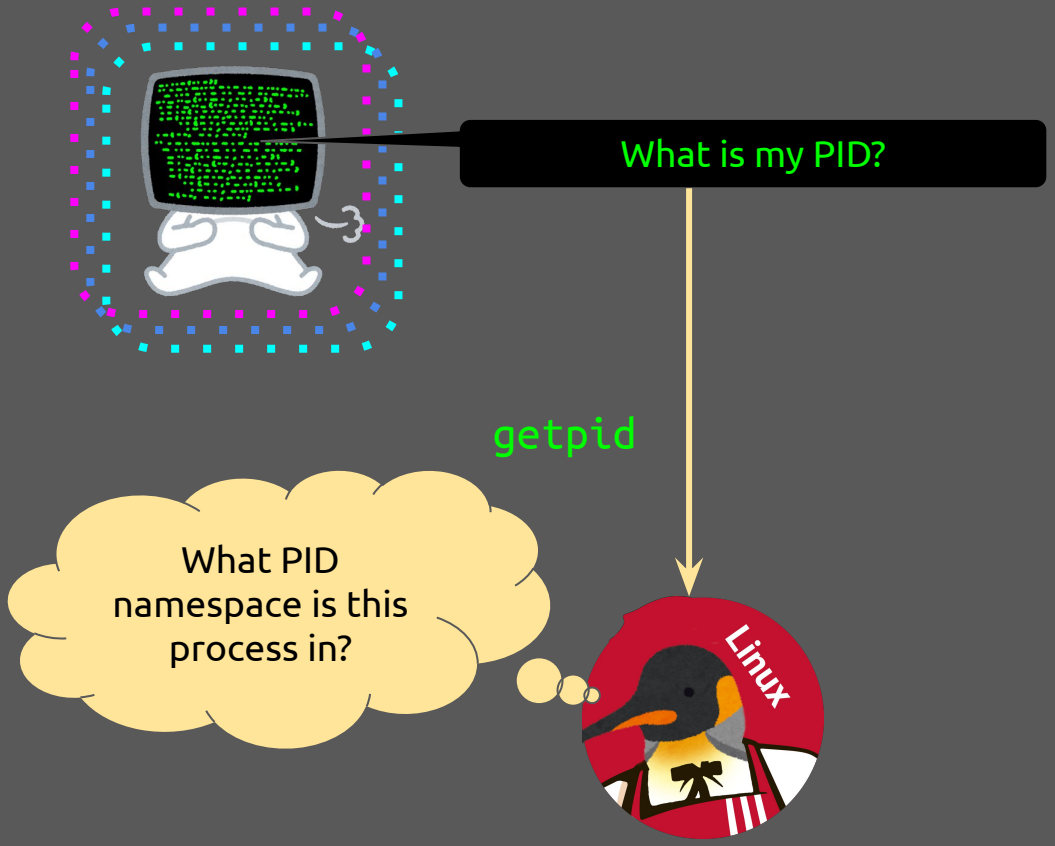

Sure!
Linux

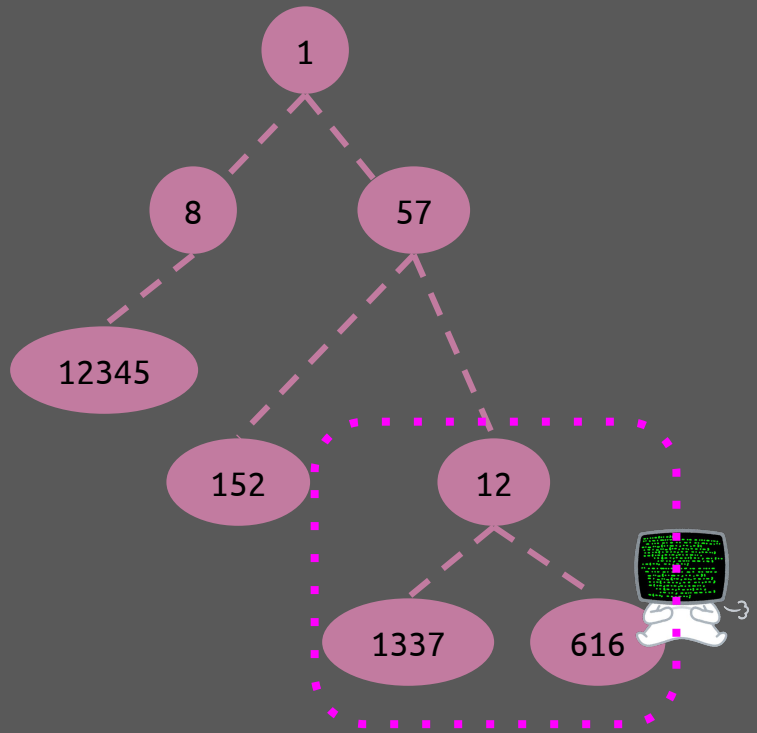

1
8
57
12345
152
12
CM

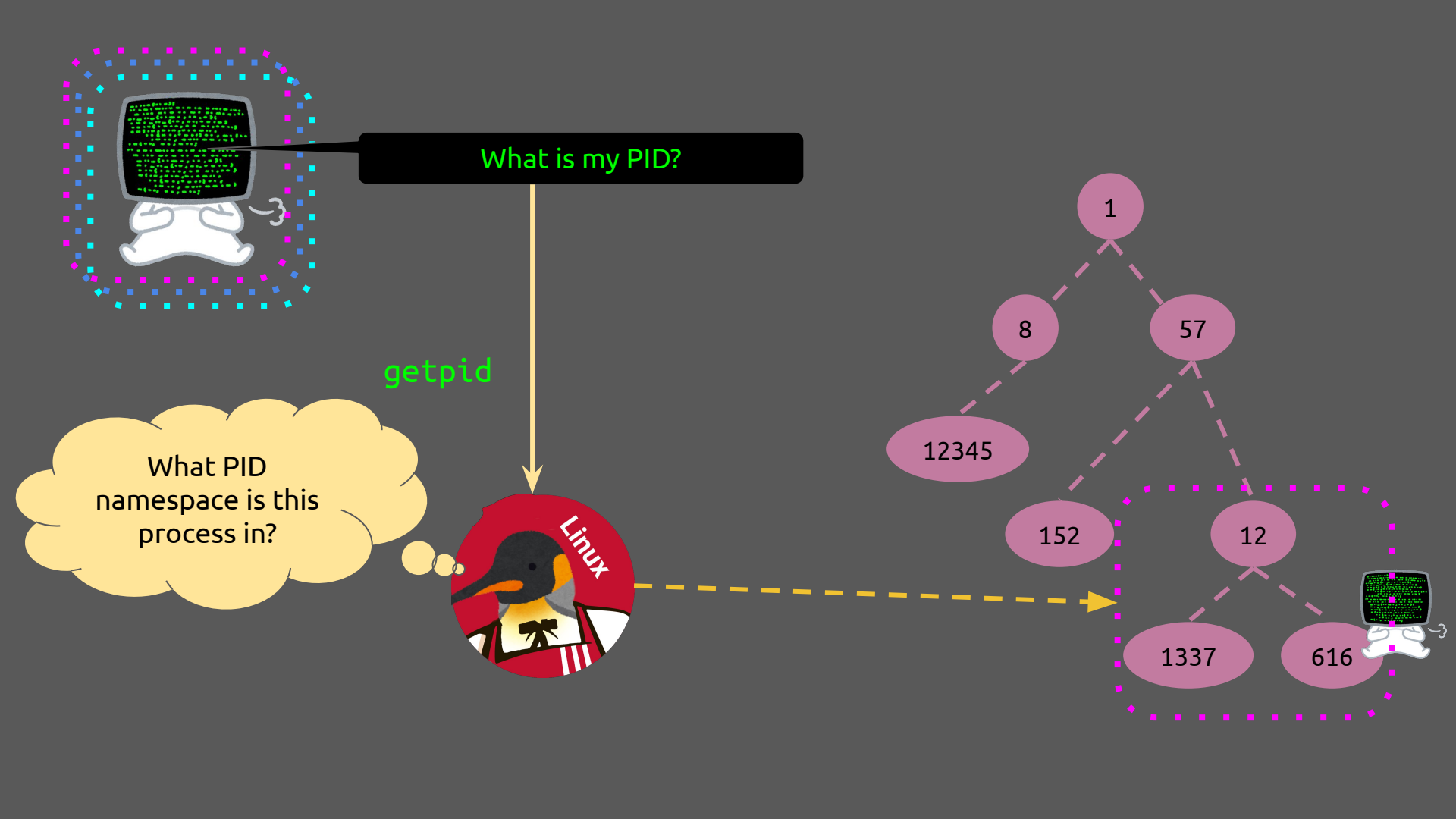

chroot("/var/www/htdocs")
unshare(CLONE_NEWNET)
unshare(CLONE_NEWPID)
...and run this process.
CM
Sure!
Linux
1
8
57
12345
152
12
1337
616

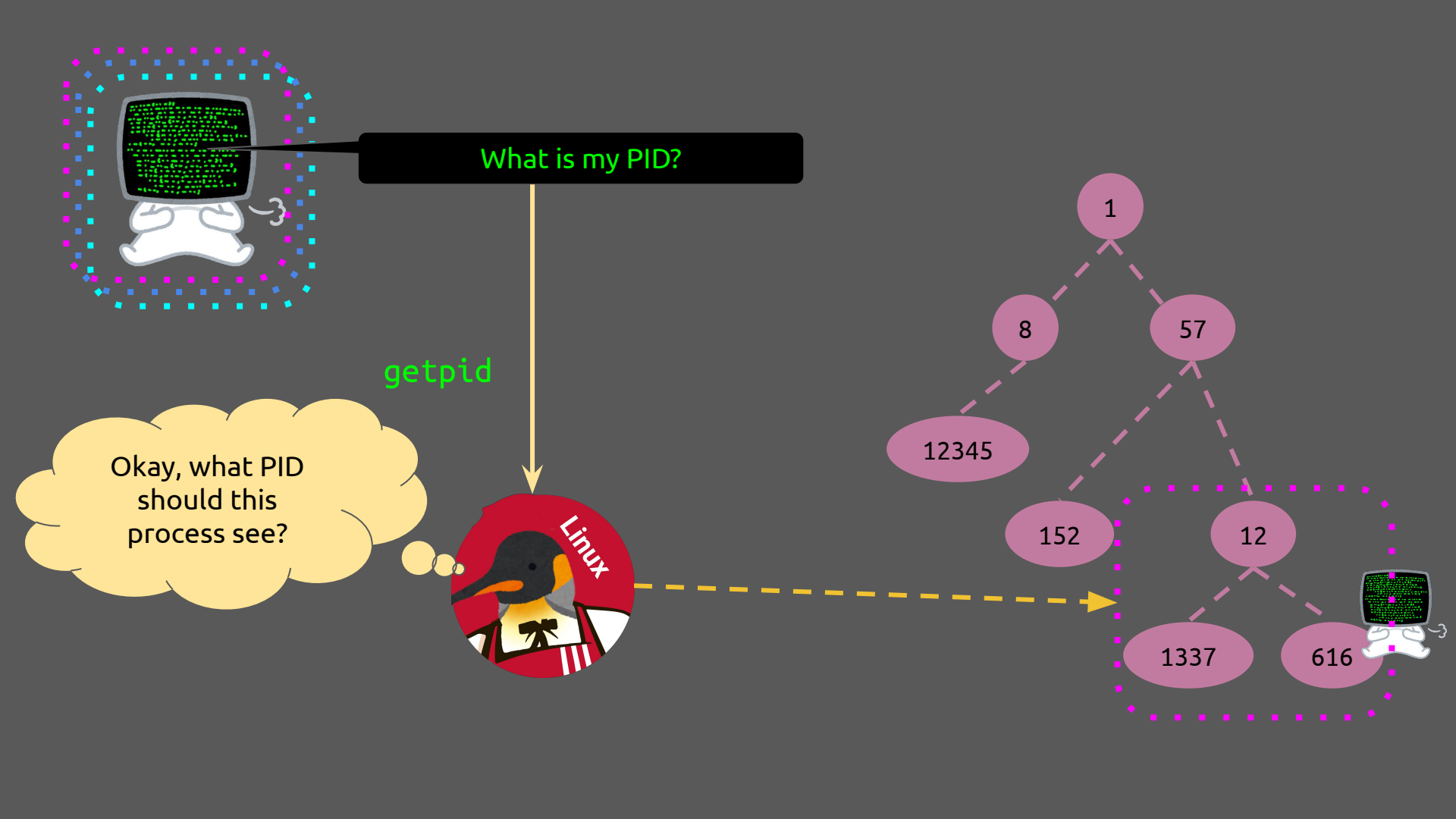

What is my PID?
getpid
Linux

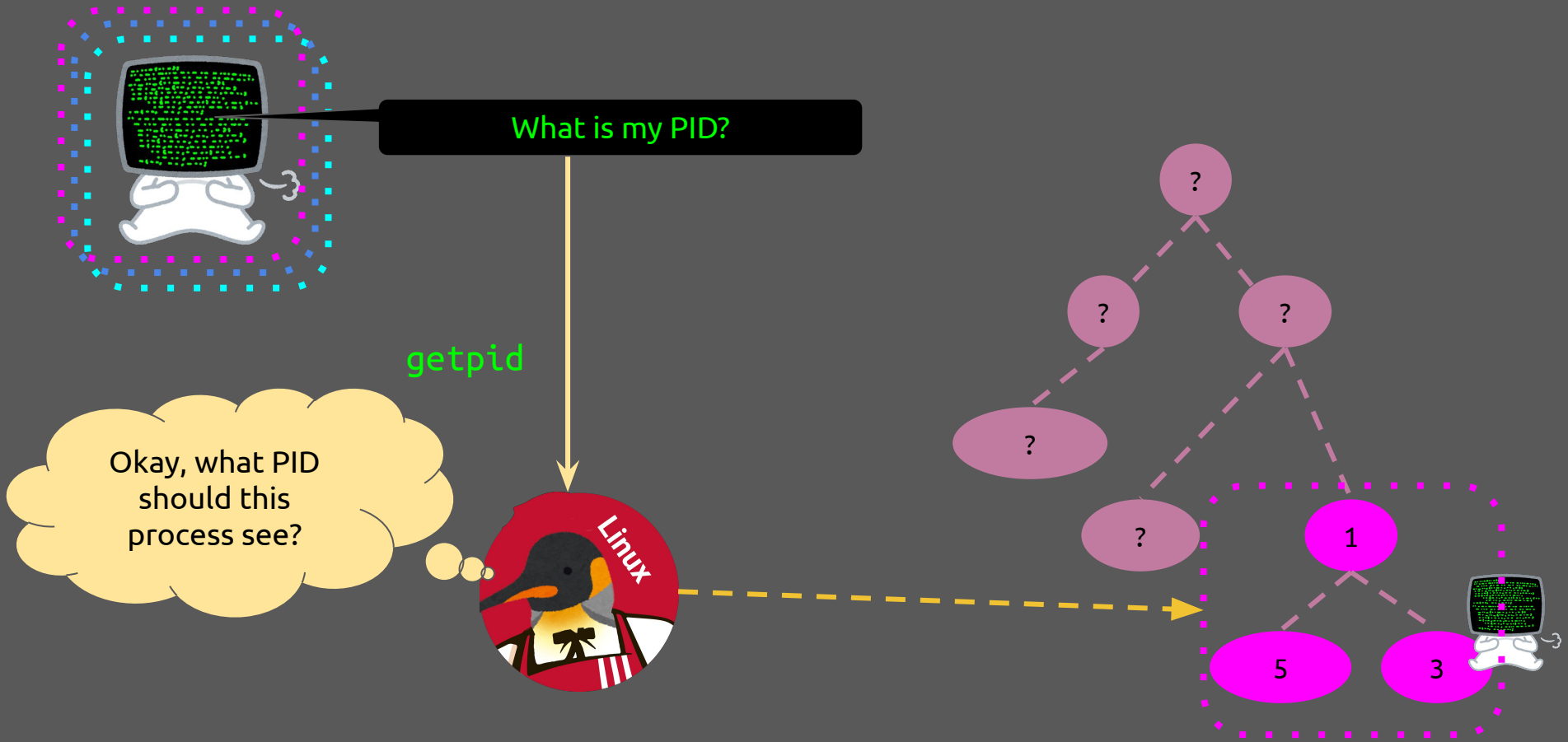

1
8
57
12345
152
12
1337
616

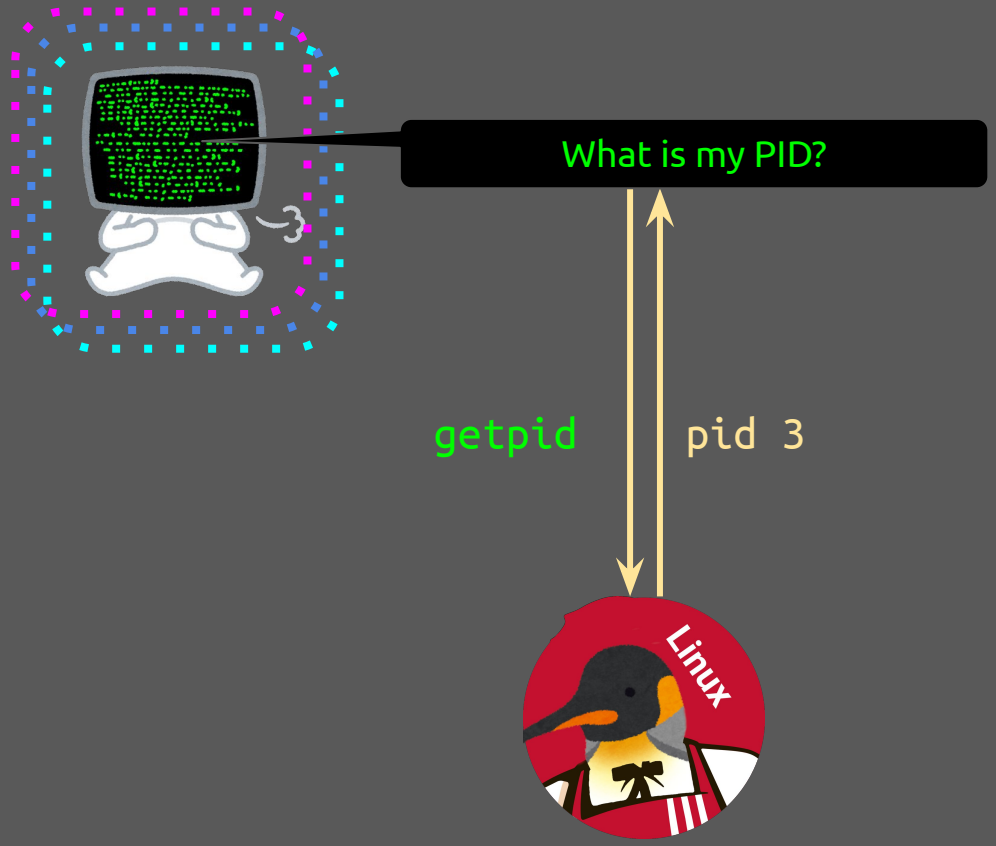

What is my PID?
getpid
What PID namespace is this process in?
Linux

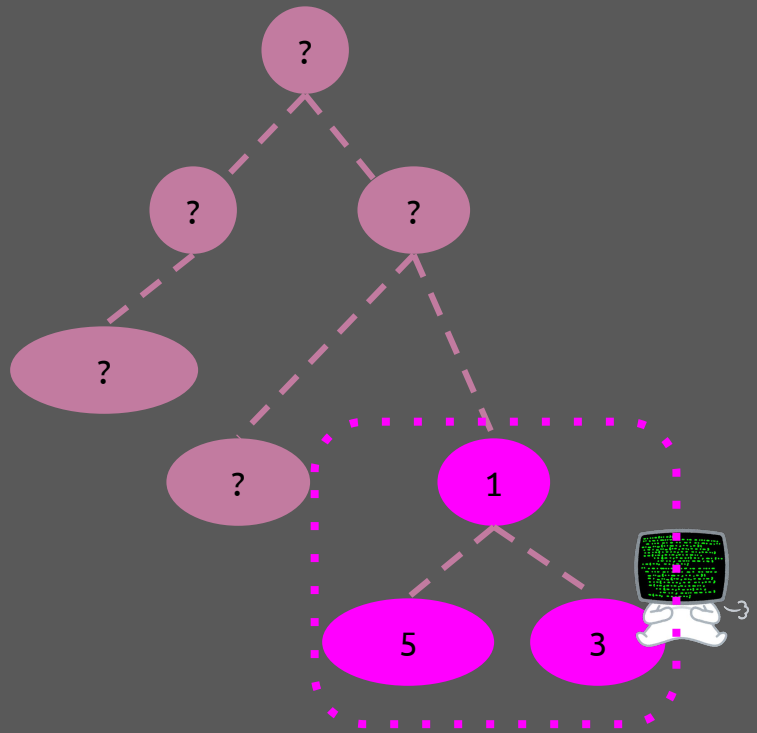

1
8
57
12345
152
12
1337
616

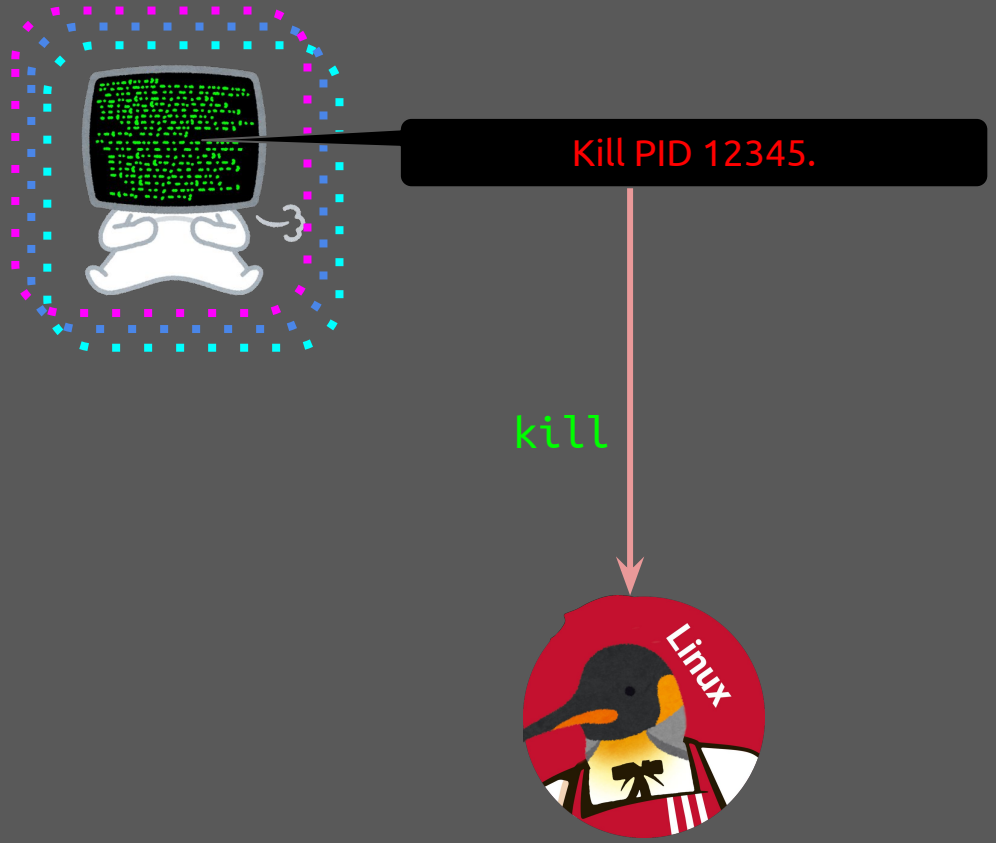

What is my PID?
getpid
What PID namespace is this process in?
Linux
1
8
57
12345
152
12
1337
616

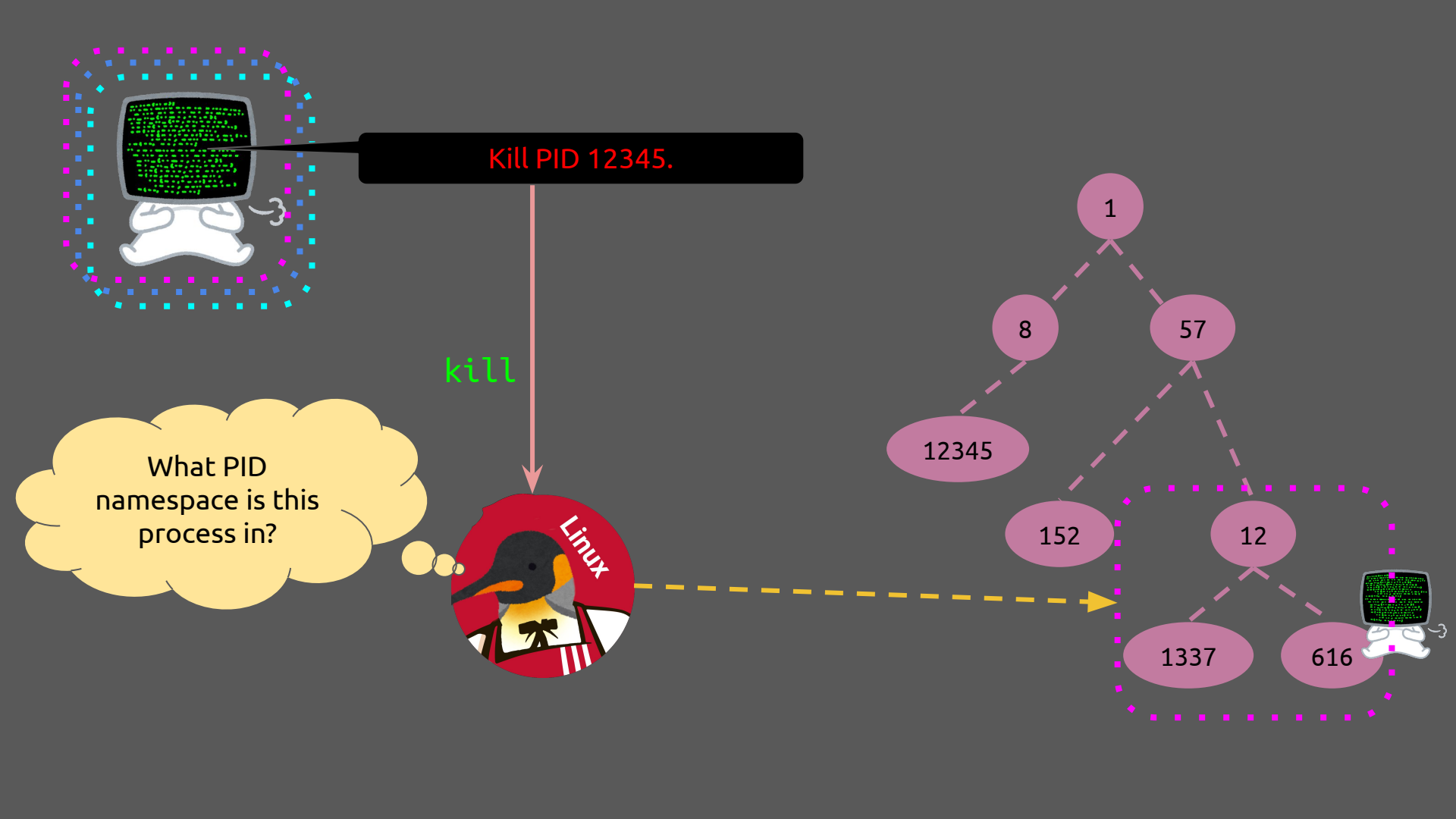

What is my PID?
getpid
Okay, what PID should this process see?
Linux
1
8
57
12345
152
12
1337
616

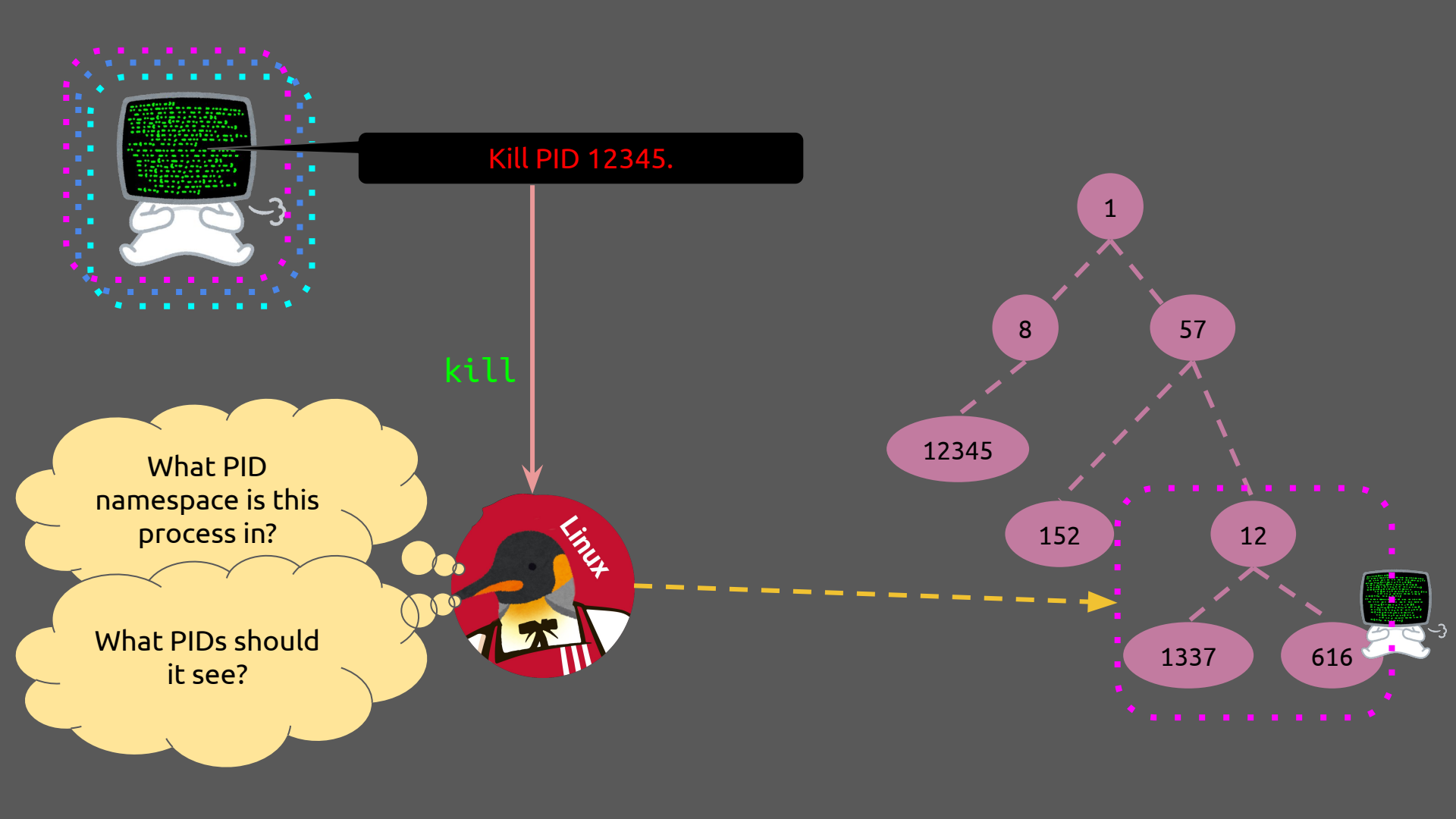

What is my PID?
getpid
Okay, what PID should this process see?
Linux
?
?
?
?
?
1
5
3

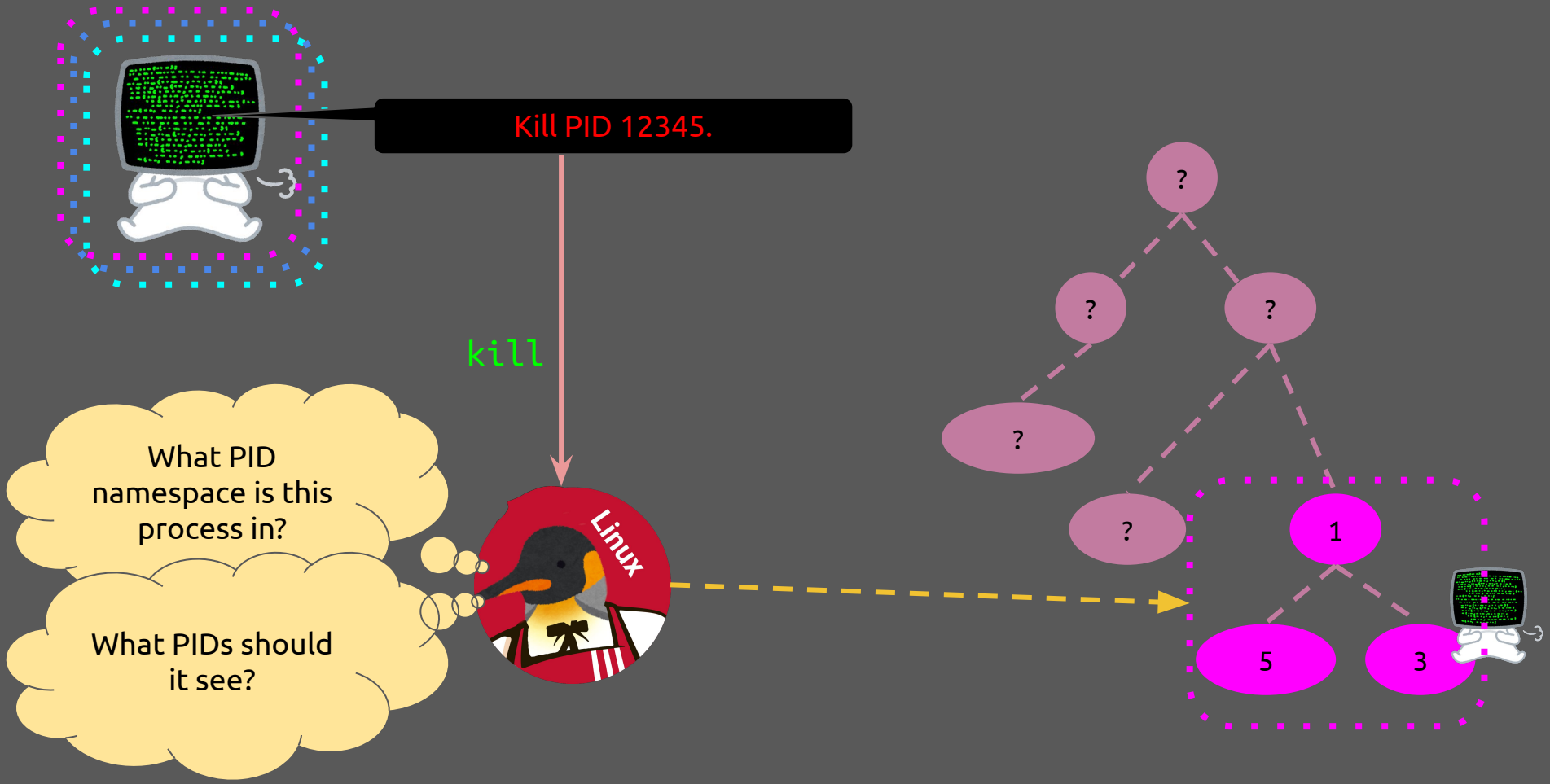

What is my PID?
getpid
pid 3
Linux

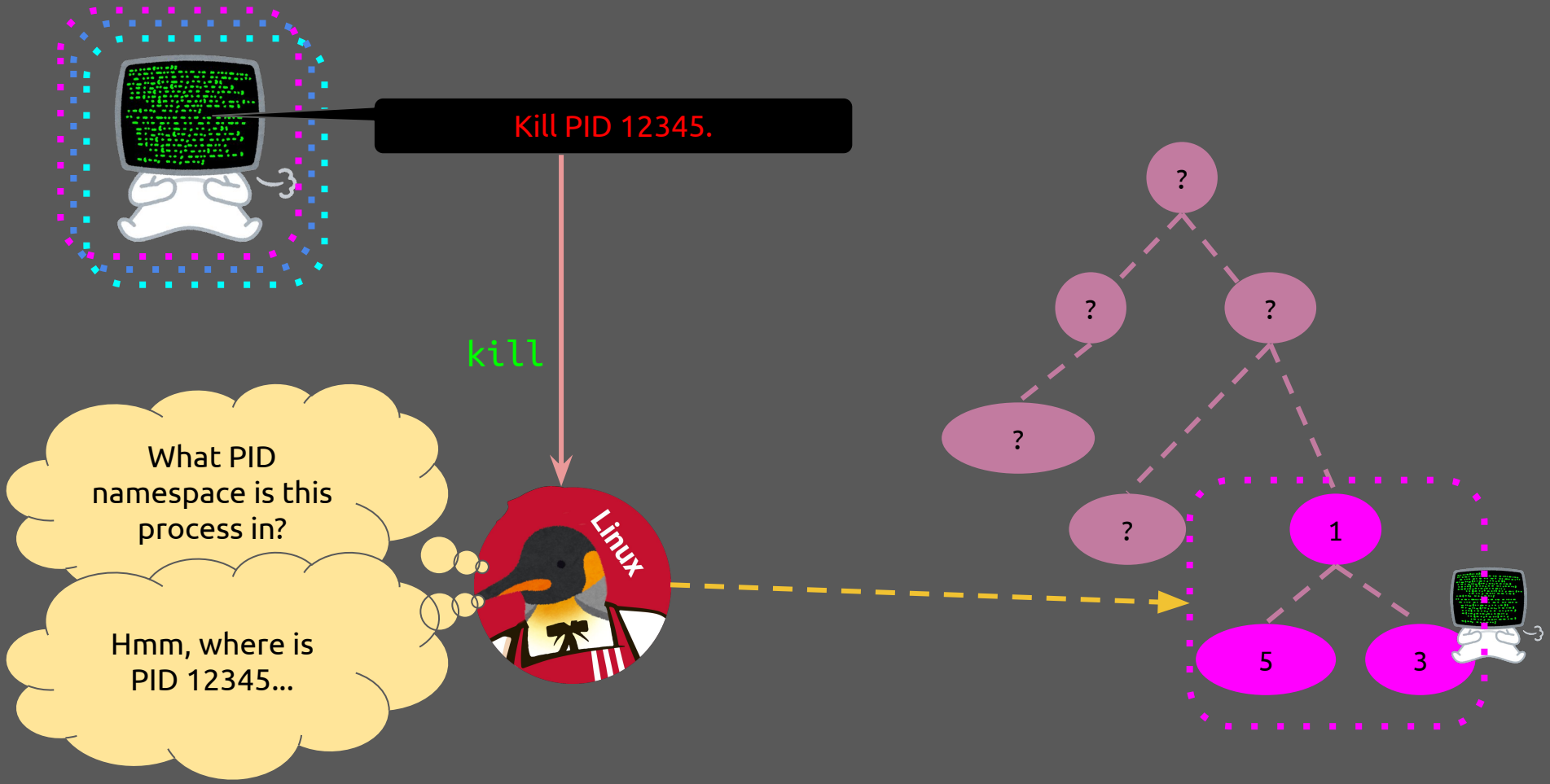

?
?
?
?
?
1
5
3

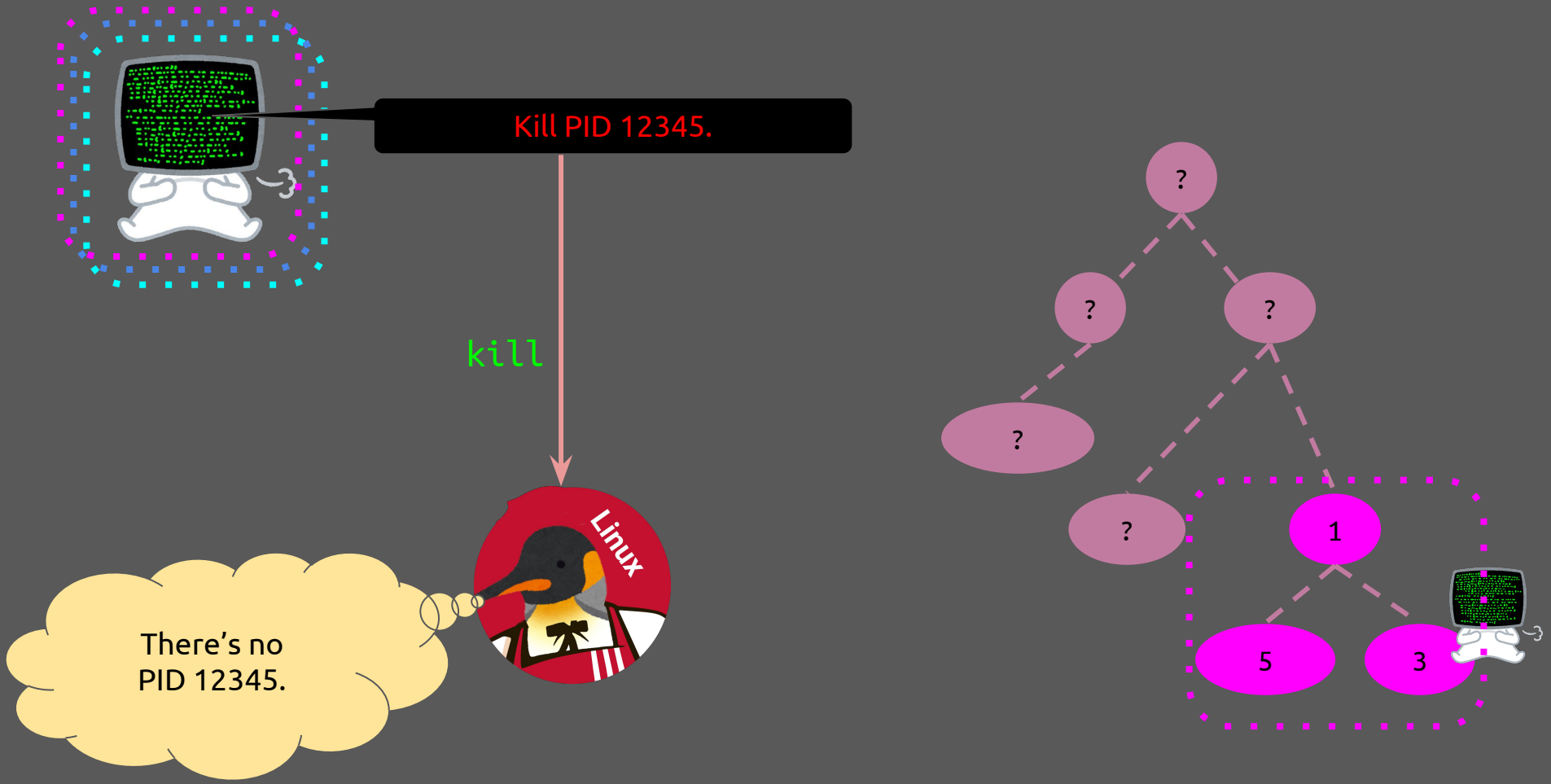

Kill PID 12345.
kill
Linux
1
8
57
12345
152
12
1337
616

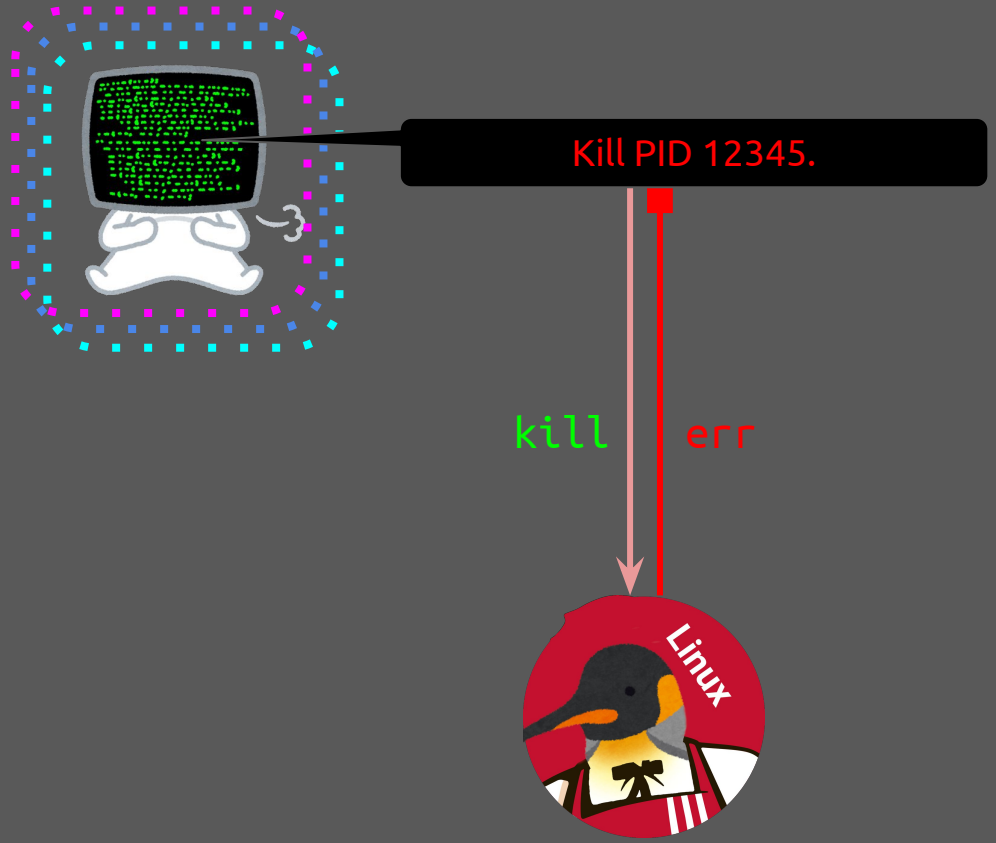

Kill PID 12345.
kill
What PID namespace is this process in?
Linux
1
8
57
12345
152
12
1337
616

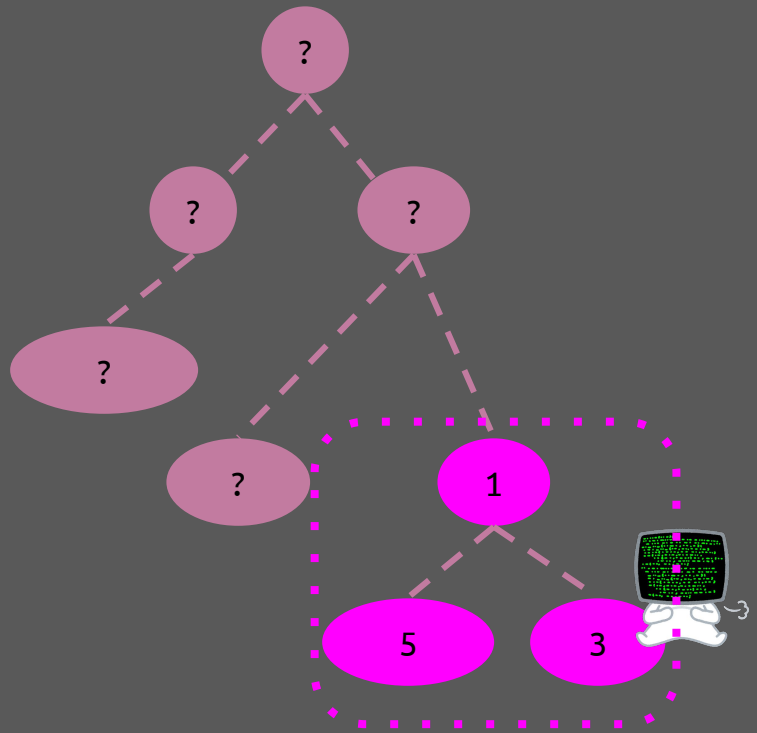

Kill PID 12345.
kill
What PID namespace is this process in?
What PIDs should it see?
Linux
1
8
57
12345
152
12
1337
616


Kill PID 12345.
kill
What PID namespace is this process in?
What PIDs should it see?
Linux
?
?
?
?
?
1
5
3


Kill PID 12345.
kill
What PID namespace is this process in?
Hmm, where is PID 12345...
Linux
?
?
?
?
?
1
5
3

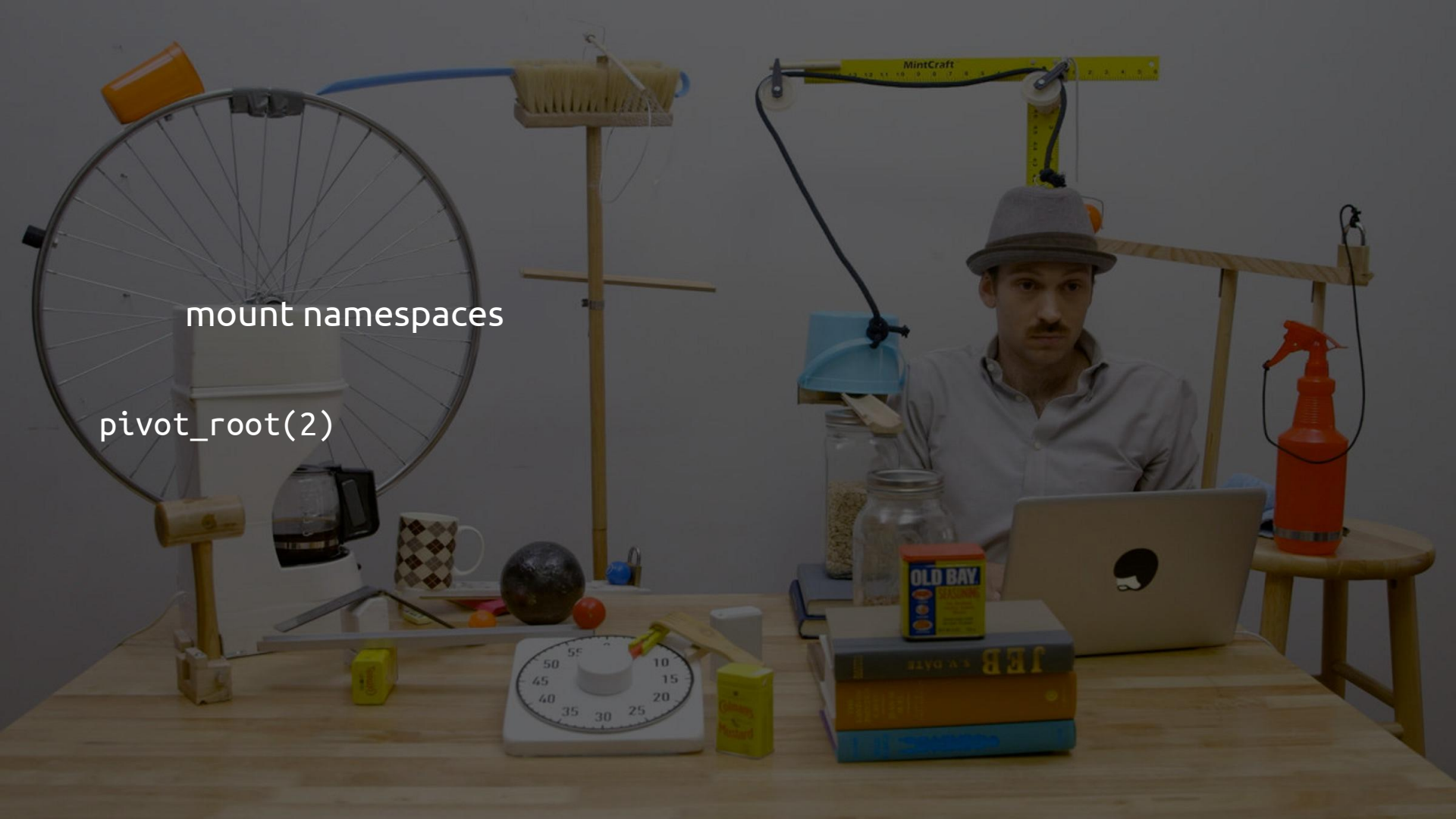

Kill PID 12345.
kill
Linux
There’s no
PID 12345.
?
?
?
?
?
1
5
3

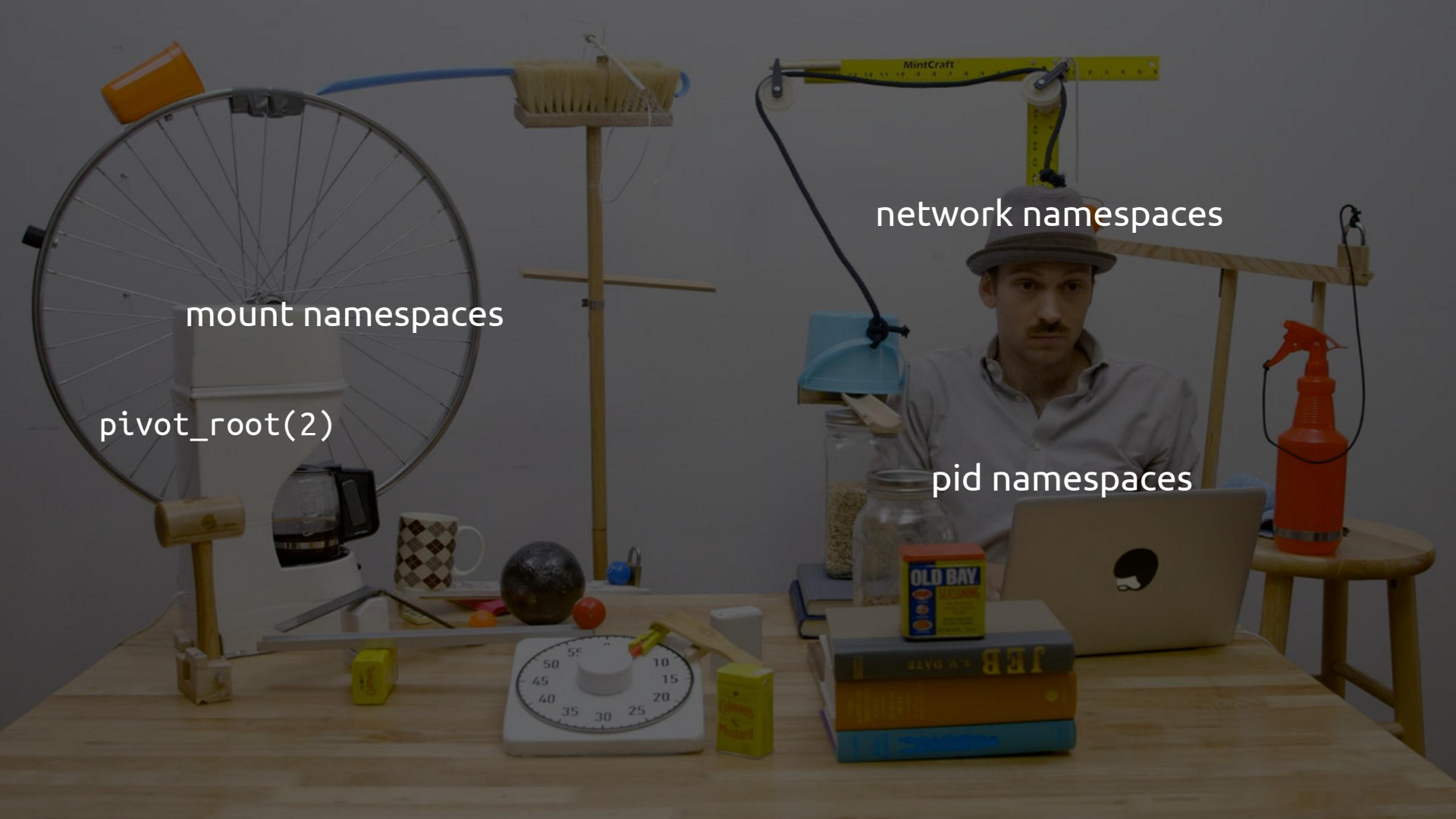

Kill PID 12345.
kill
err
Linux

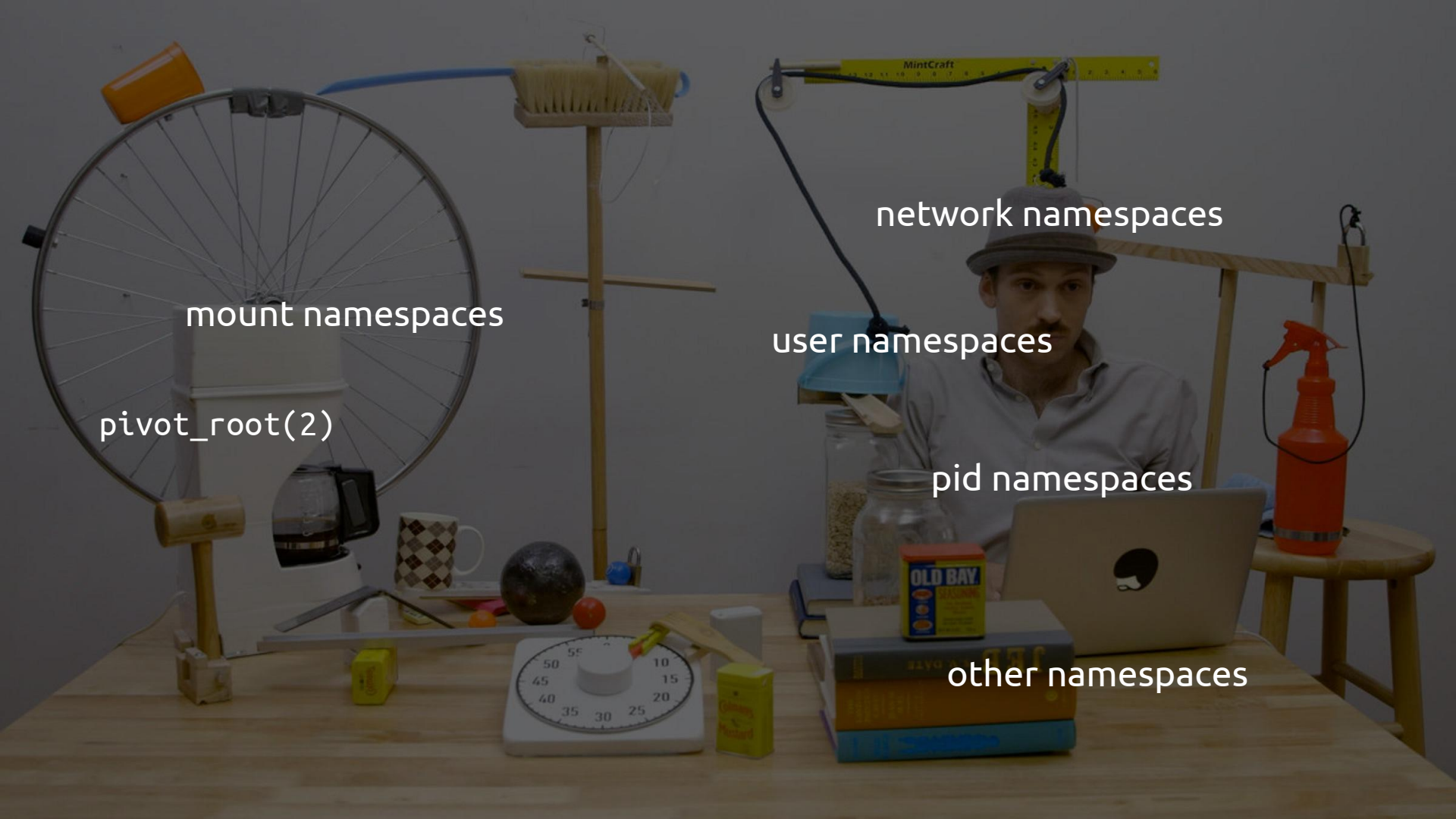

?
?
?
?
?
1
5
3

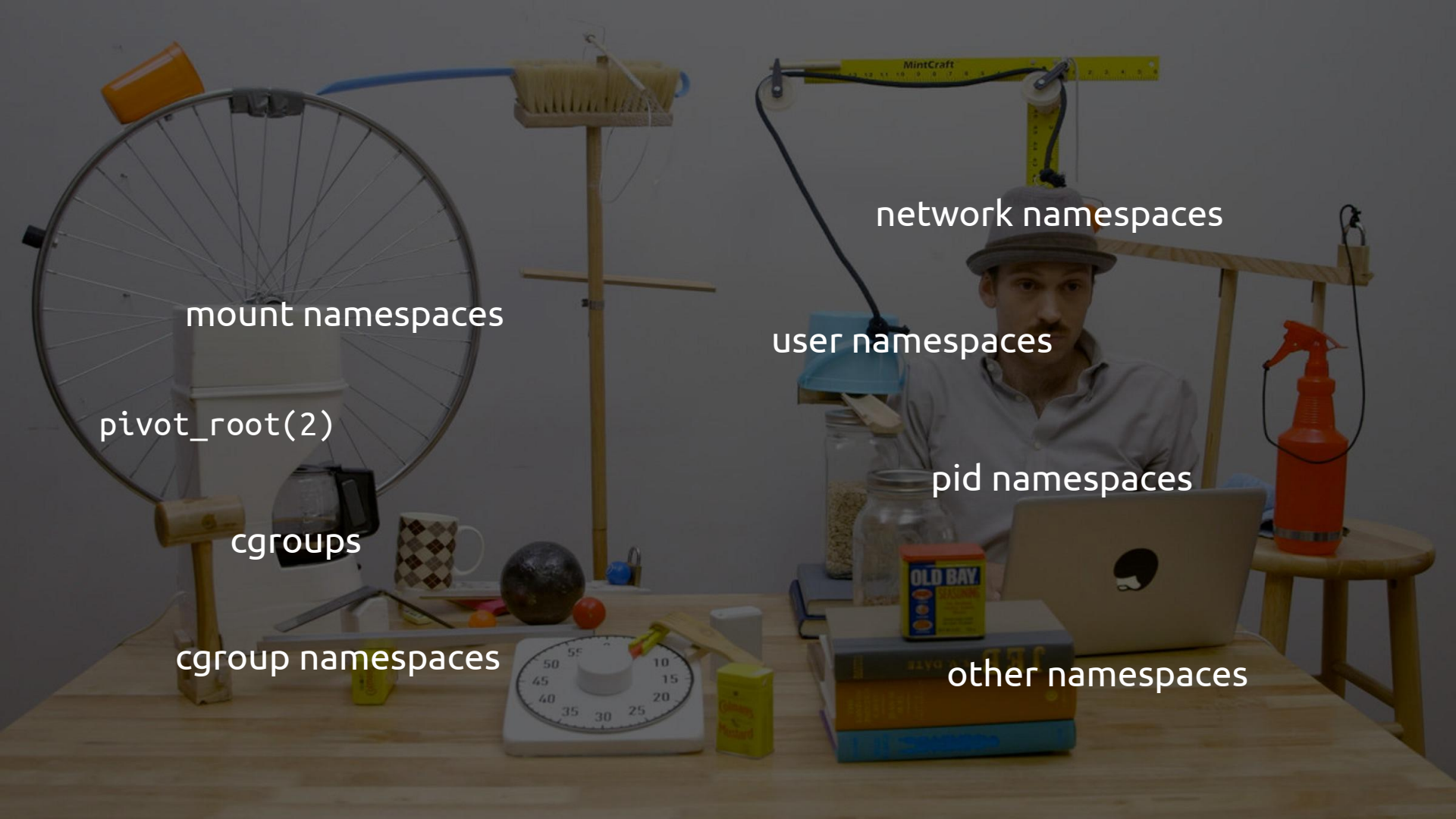

MintCraft
OLD BAY
JEB

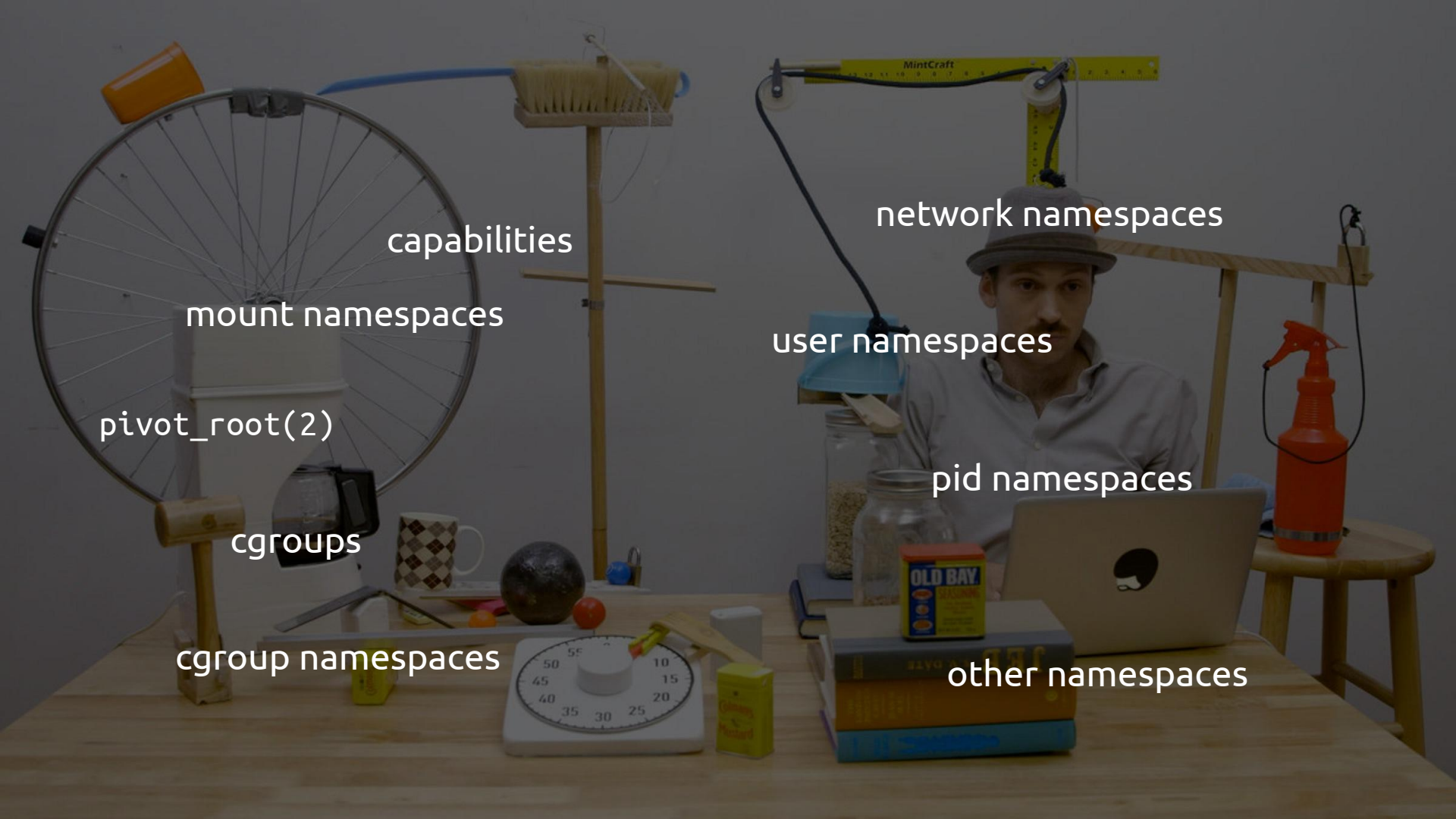
chroot(2)

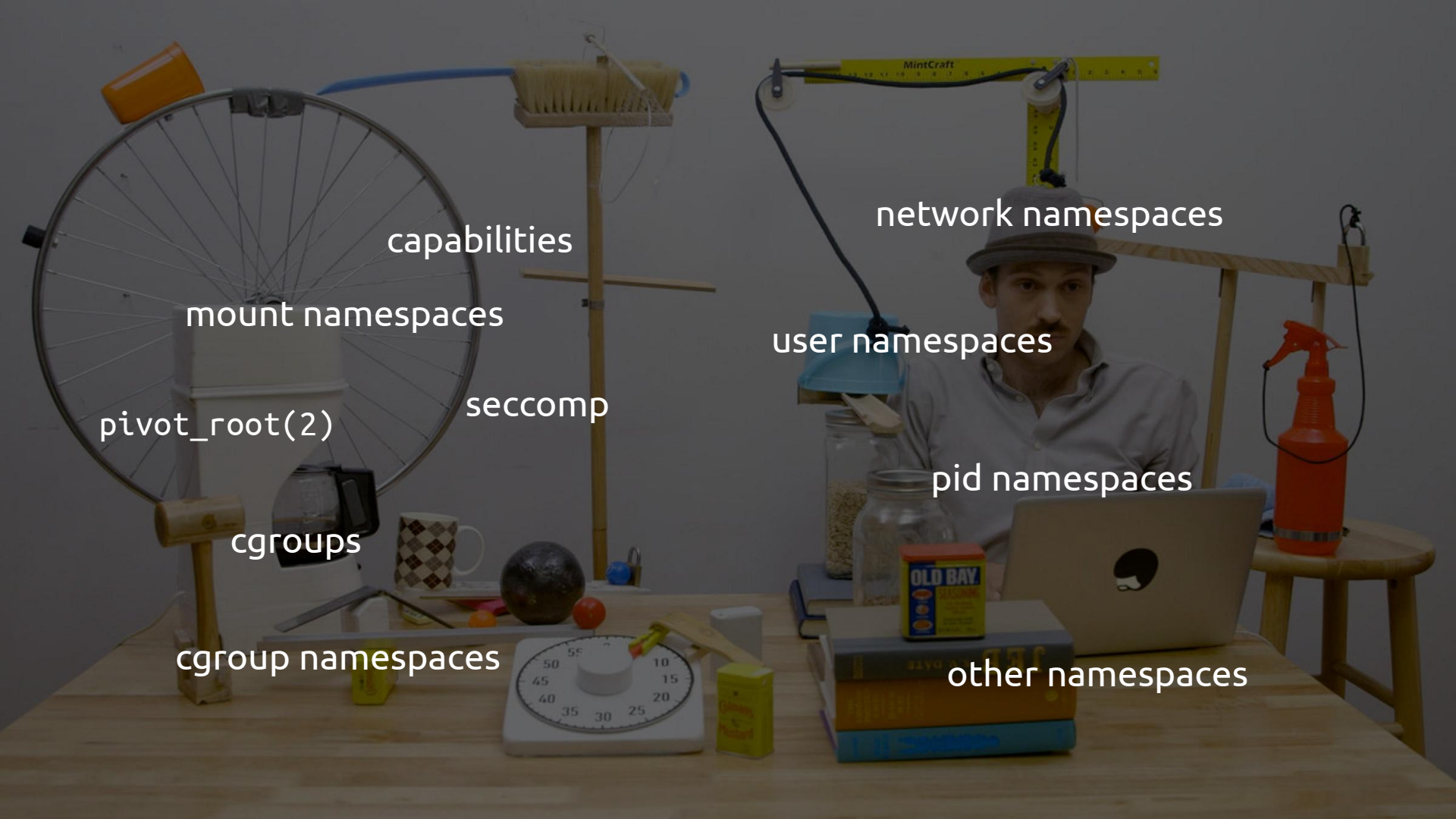

mount namespaces
pivot_root(2)
MintCraft
OLD BAY

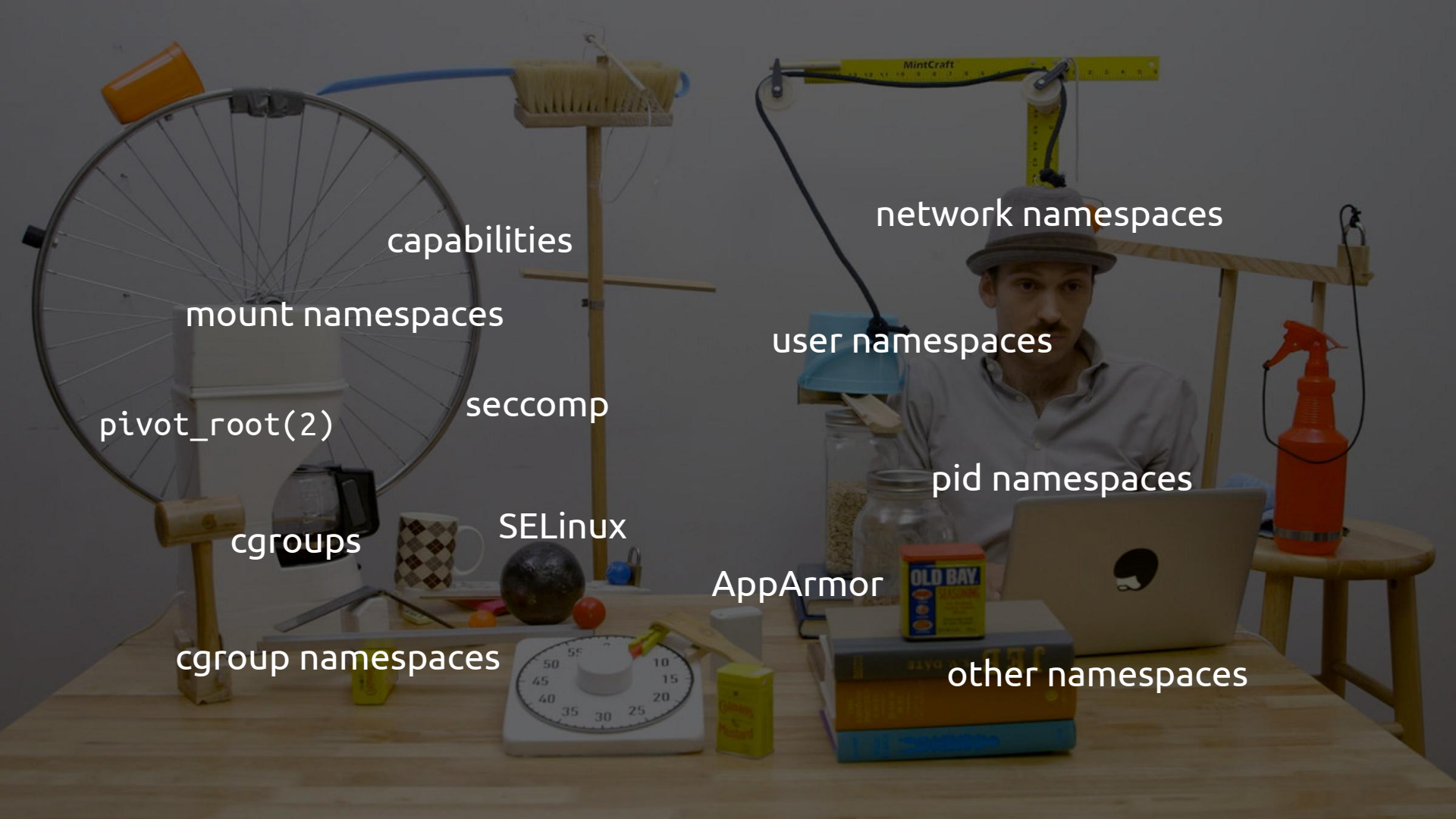

network namespaces
mount namespaces
pivot_root(2)
pid namespaces
MintCraft
OLD BAY

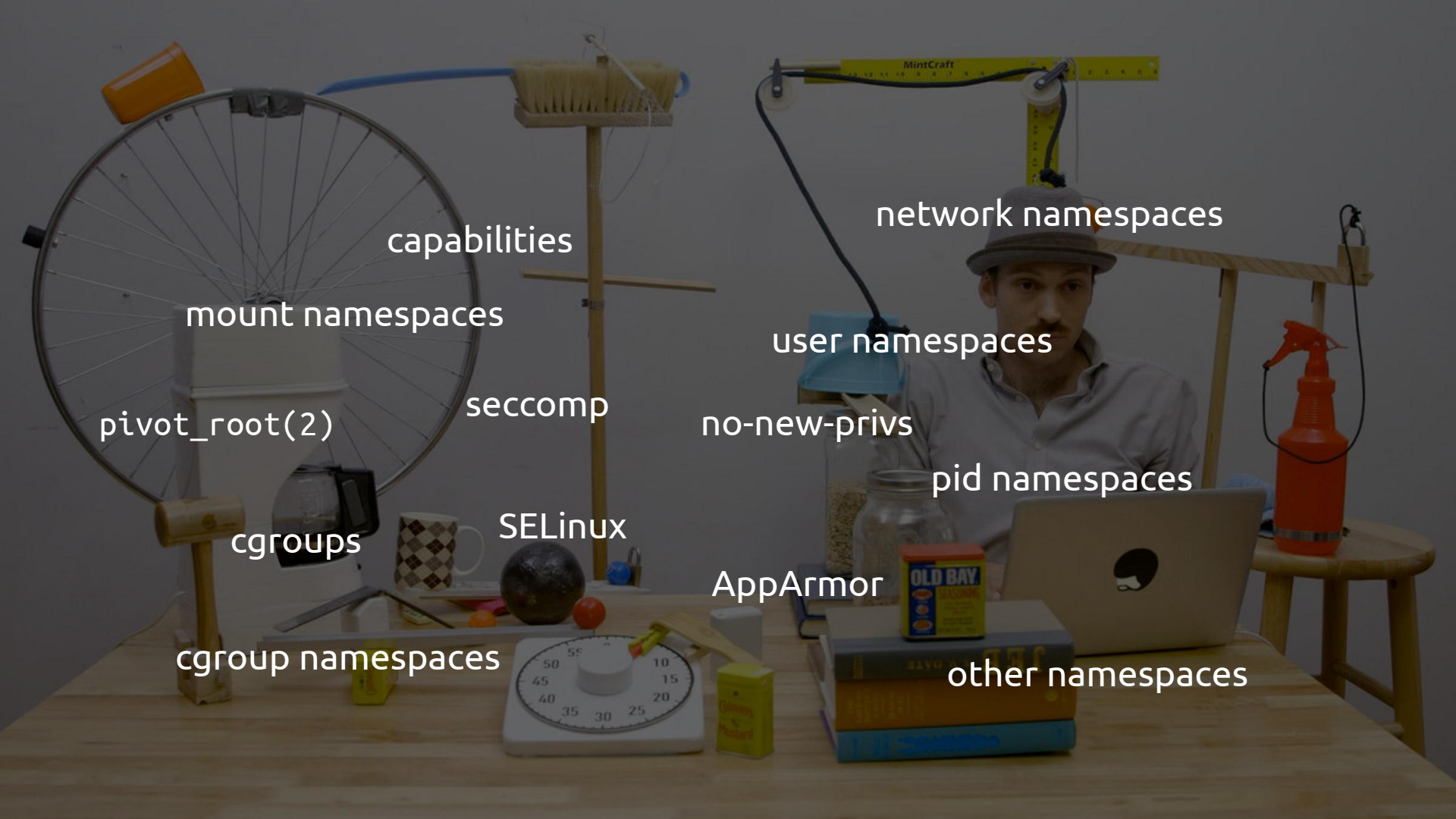

network namespaces
mount namespaces
user namespaces
pivot_root(2)
pid namespaces
other namespaces

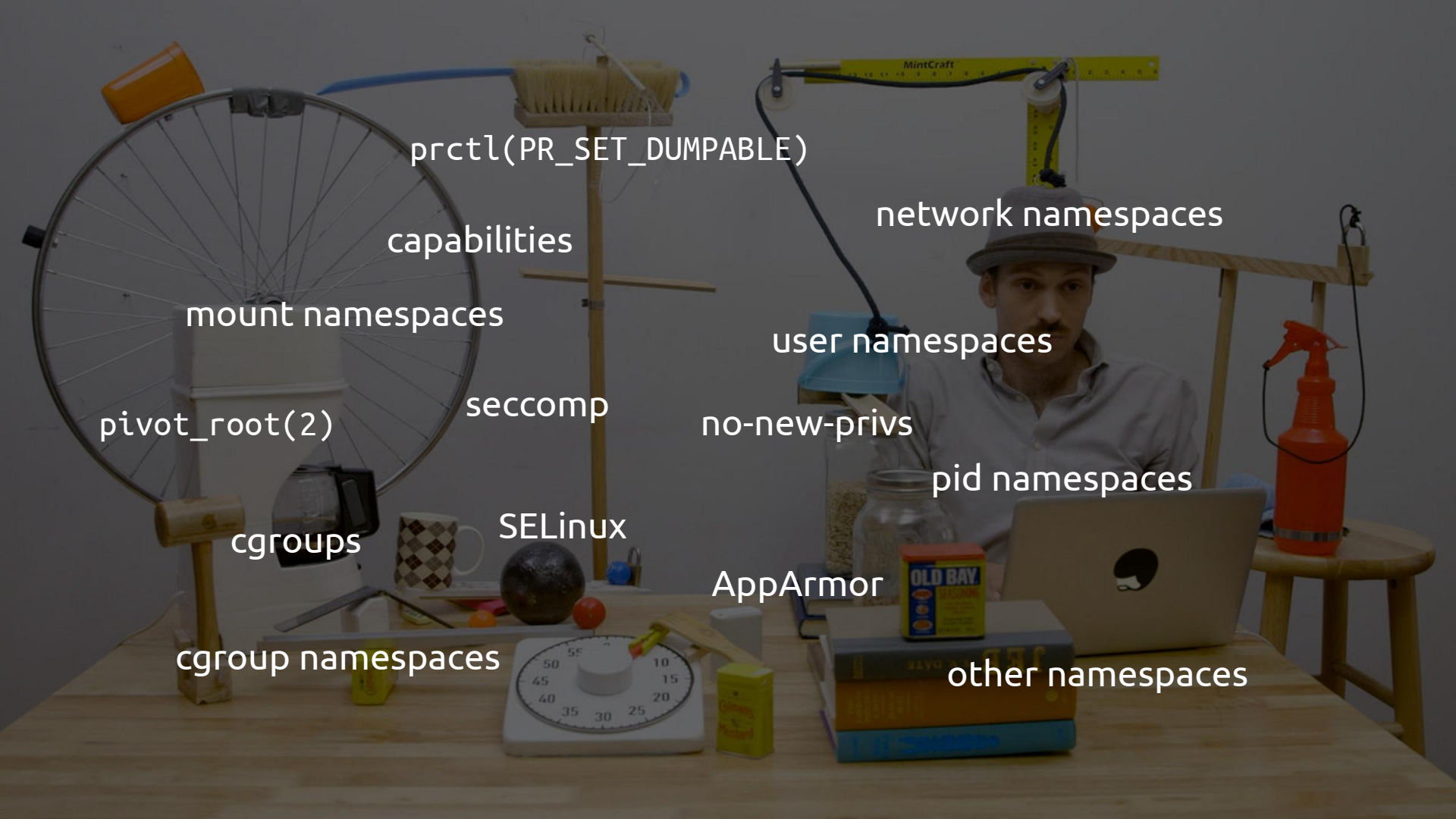

network namespaces
mount namespaces
user namespaces
pivot_root(2)
pid namespaces
cgroups
cgroup namespaces
other namespaces

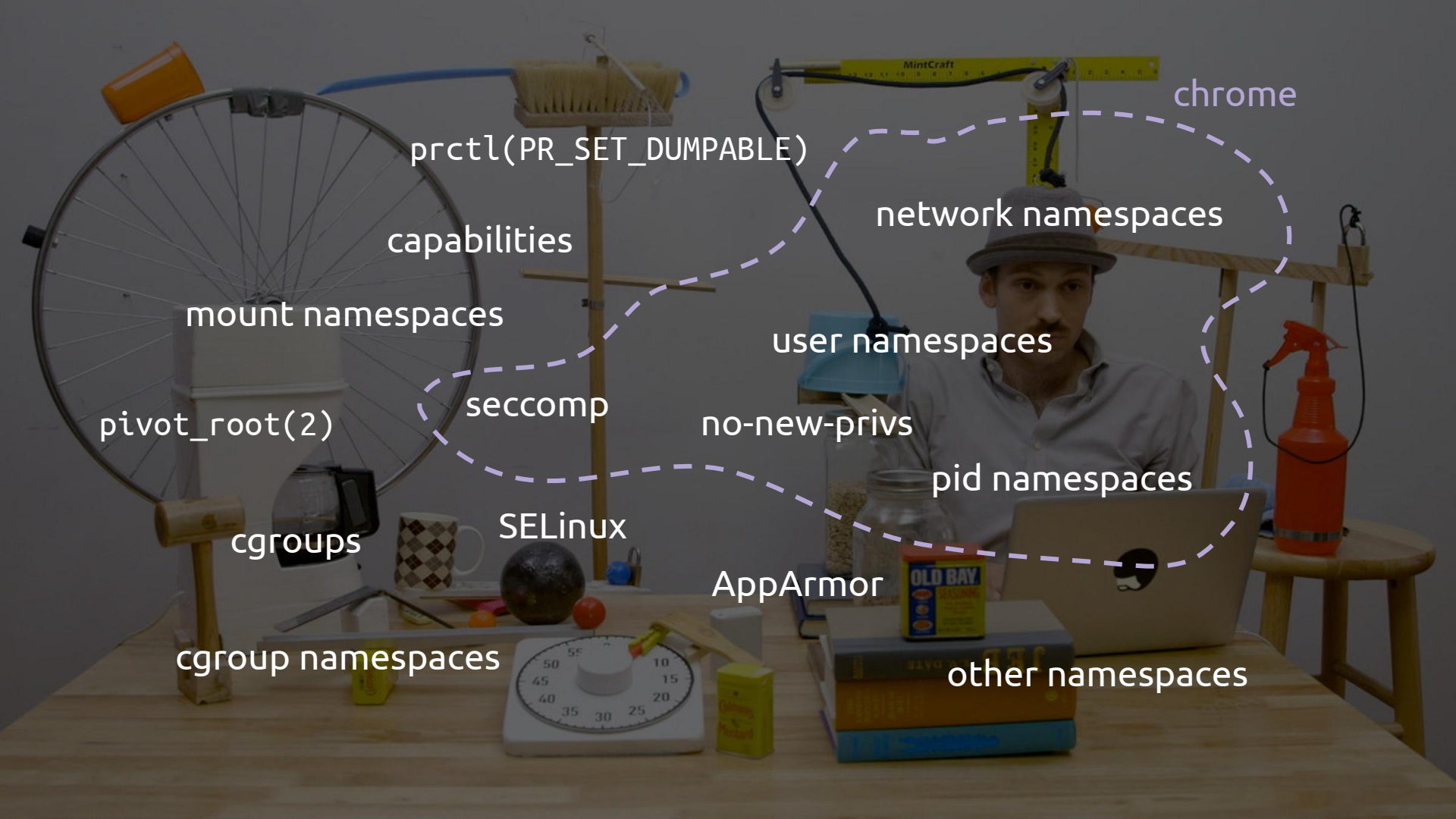

capabilities
mount namespaces
pivot_root(2)
cgroups
cgroup namespaces
network namespaces
user namespaces
pid namespaces
other namespaces
MintCraft
OLD BAY

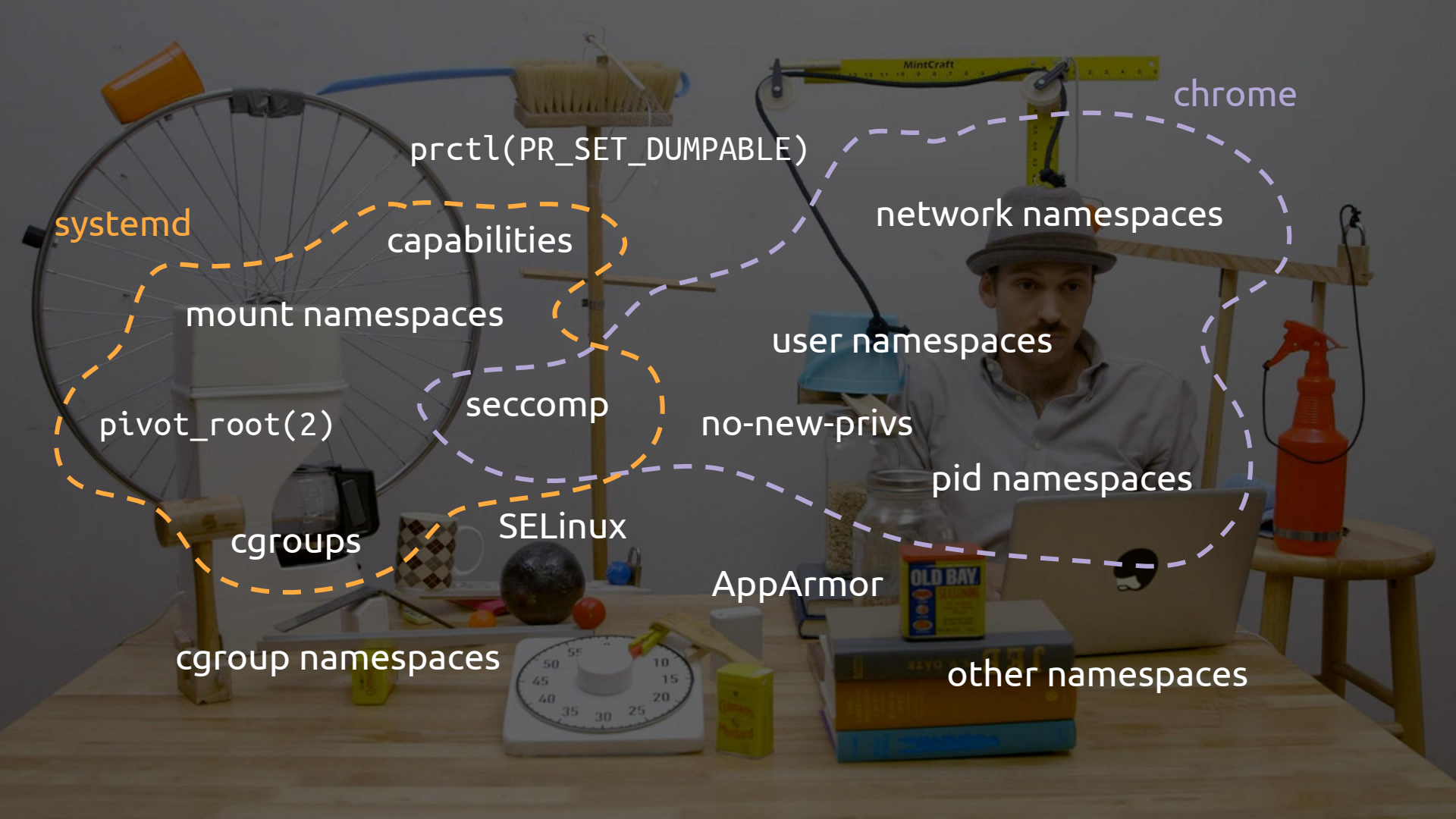

capabilities
mount namespaces
pivot_root(2)
seccomp
cgroups
cgroup namespaces
network namespaces
user namespaces
pid namespaces
other namespaces
MintCraft
OLD BAY

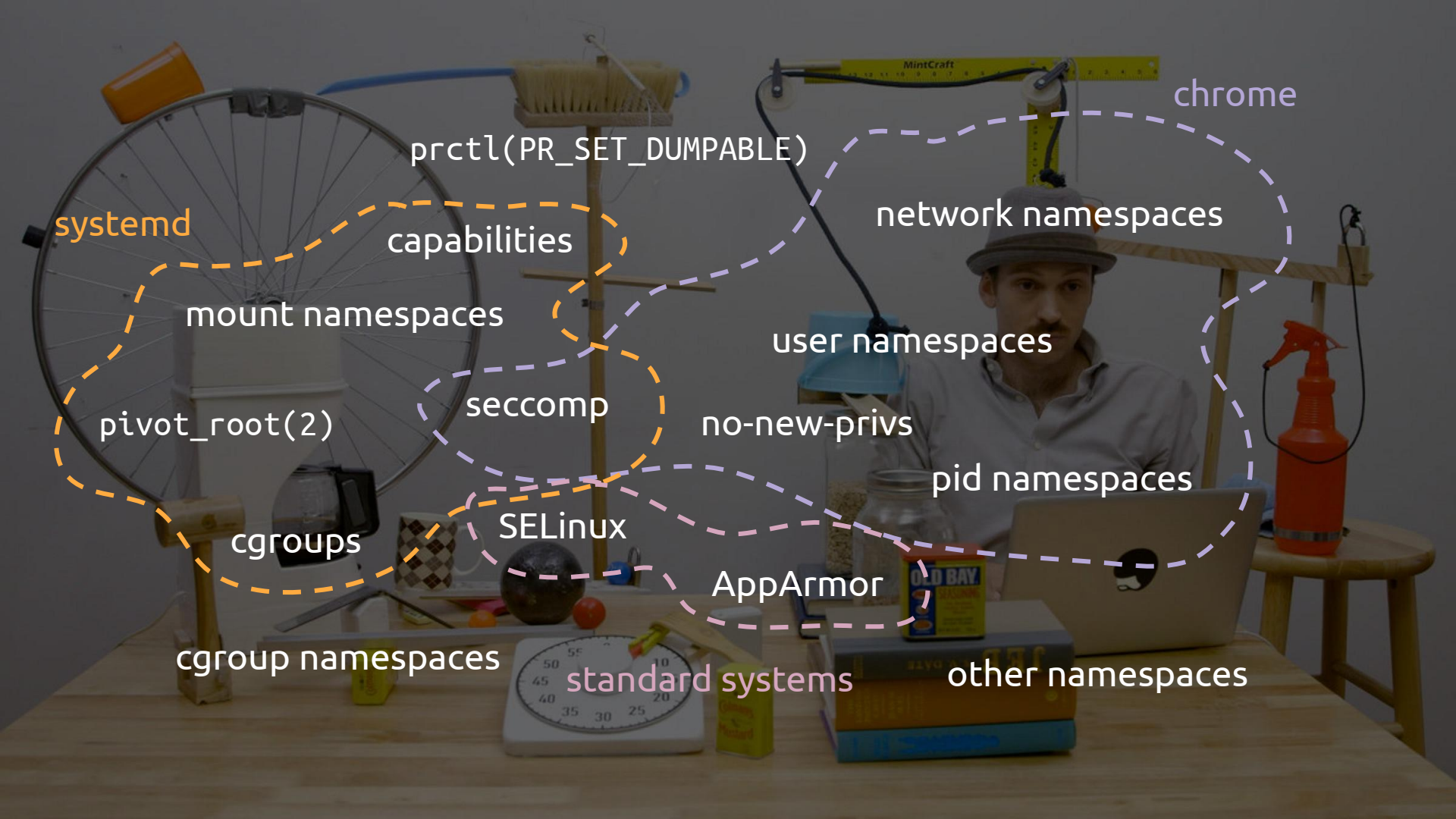

capabilities
mount namespaces
pivot_root(2)
seccomp
cgroups
SELinux
cgroup namespaces
network namespaces
user namespaces
pid namespaces
AppArmor
other namespaces

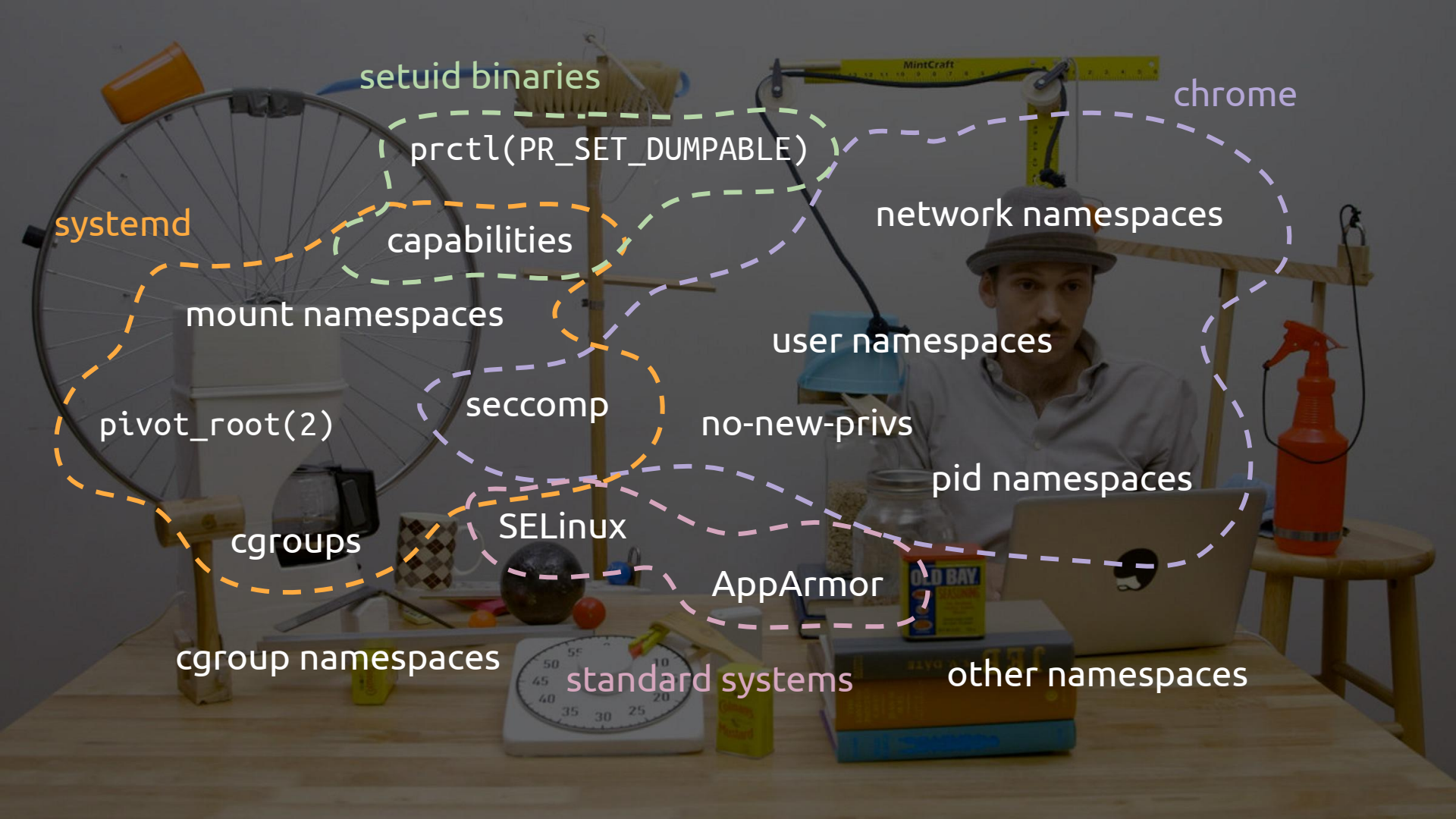

capabilities
mount namespaces
pivot_root(2)
seccomp
cgroups
SELinux
cgroup namespaces
network namespaces
user namespaces
no-new-privs
pid namespaces
AppArmor
other namespaces
MintCraft
OLD BAY

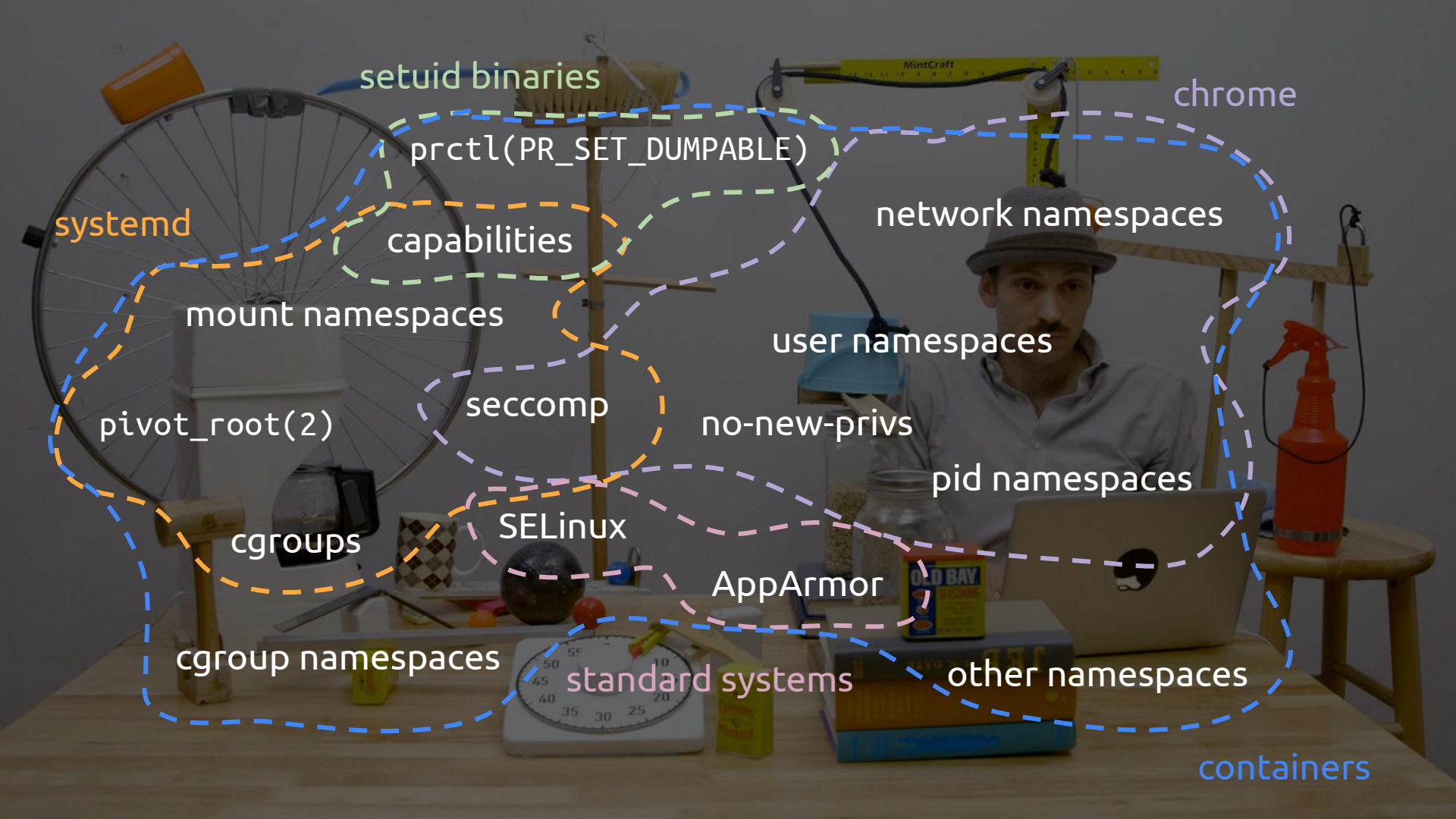

prctl(PR_SET_DUMPABLE)
capabilities
network namespaces
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
other namespaces

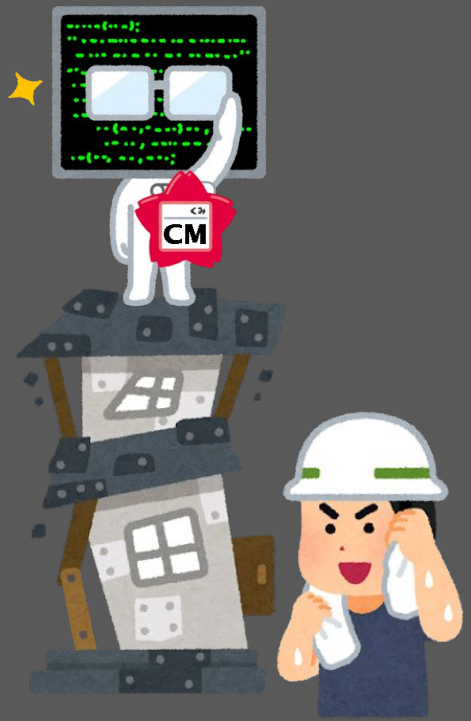

chrome
prctl(PR_SET_DUMPABLE)
network namespaces
capabilities
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
other namespaces


chrome
prctl(PR_SET_DUMPABLE)
systemd
capabilities
network namespaces
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
other namespaces


chrome
prctl(PR_SET_DUMPABLE)
systemd
capabilities
network namespaces
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
standard systems
other namespaces


setuid binaries
prctl(PR_SET_DUMPABLE)
chrome
systemd
capabilities
network namespaces
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
standard systems
other namespaces


setuid binaries
chrome
prctl(PR_SET_DUMPABLE)
systemd
capabilities
network namespaces
mount namespaces
user namespaces
seccomp
pivot_root(2)
no-new-privs
pid namespaces
SELinux
cgroups
AppArmor
cgroup namespaces
standard systems
other namespaces
containers

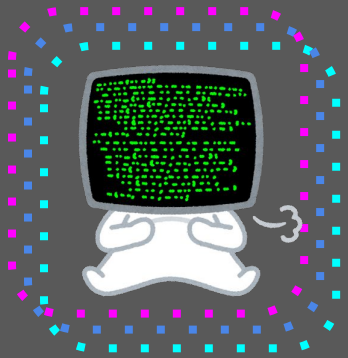

CM


A new foe has appe
CHALLENGER APPROACH
CM

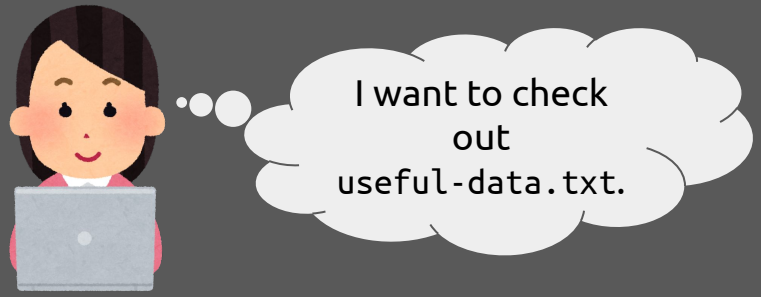

CM


CM

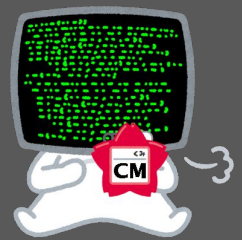
Admin

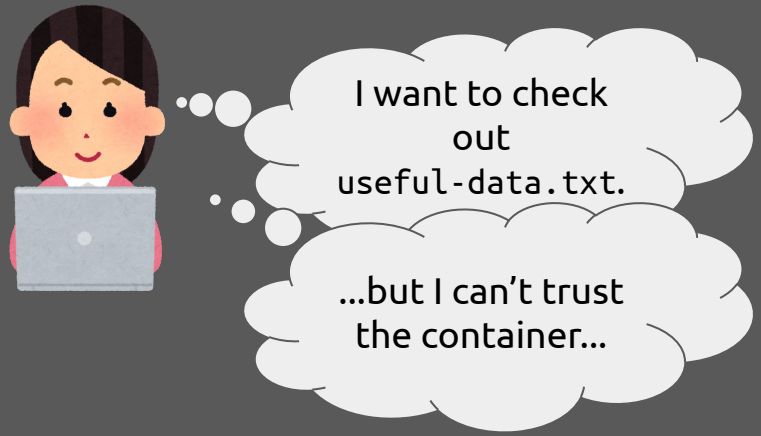



```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```




```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```






```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```

Hey, container manager!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```

Hey, container manager!

Can you get `useful-data.txt` for me?

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```

Hey, container manager!

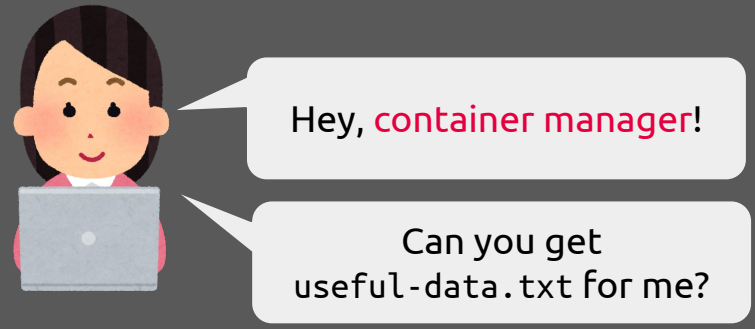
Can you get `useful-data.txt` for me?


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```

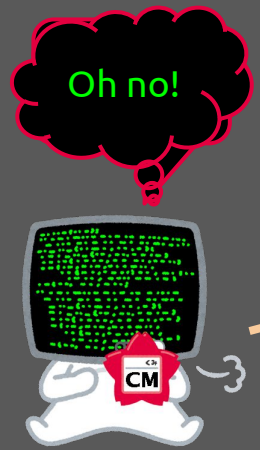
Hey, container manager!

Can you get `useful-data.txt` for me?


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```




```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```



They always forget about symlinks!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            └── files
                └── music.mp3
```


```
/
├
│
├
│
└
    ├── upload.php
    ├── useful-data.txt -> /etc/shadow
    └── files
        └── music.mp3
```

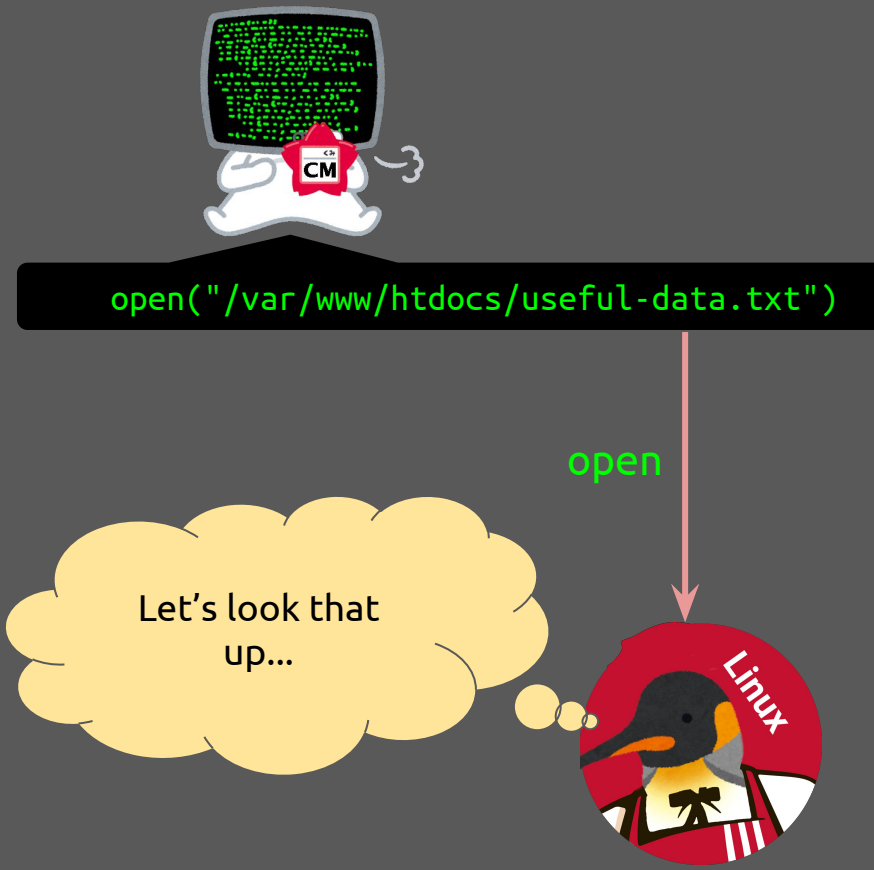

```
open("/var/www/htdocs/useful-data.txt")
```

open

Let's look that up...


```
/var/www/htdocs/useful-data.txt
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```



/var/www/htdocs/useful-data.txt

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```


```
open("/var/www/htdocs/useful-data.txt")
```

open

Let's look that up...

Ah, this points to /etc/shadow.


```
/var/www/htdocs/useful-data.txt
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```


```
open("/var/www/htdocs/useful-data.txt")
```

open

Let's look that up...

Ah, this points to /etc/shadow.

/etc/shadow

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```


```
open("/var/www/htdocs/useful-data.txt")
```

open

Let's look that up...


```
/etc/shadow
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```


```
open("/var/www/htdocs/useful-data.txt")
```

open

Let's look that up...

Ah, this points to ../../../foo.


```
/var/www/htdocs/useful-data.txt
```

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```


```
open("/var/www/htdocs/useful-data.txt")
```

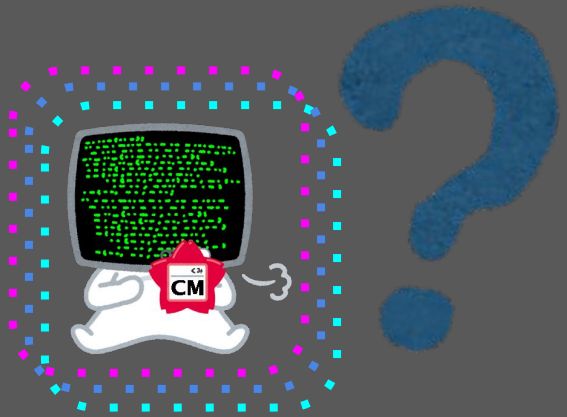
open

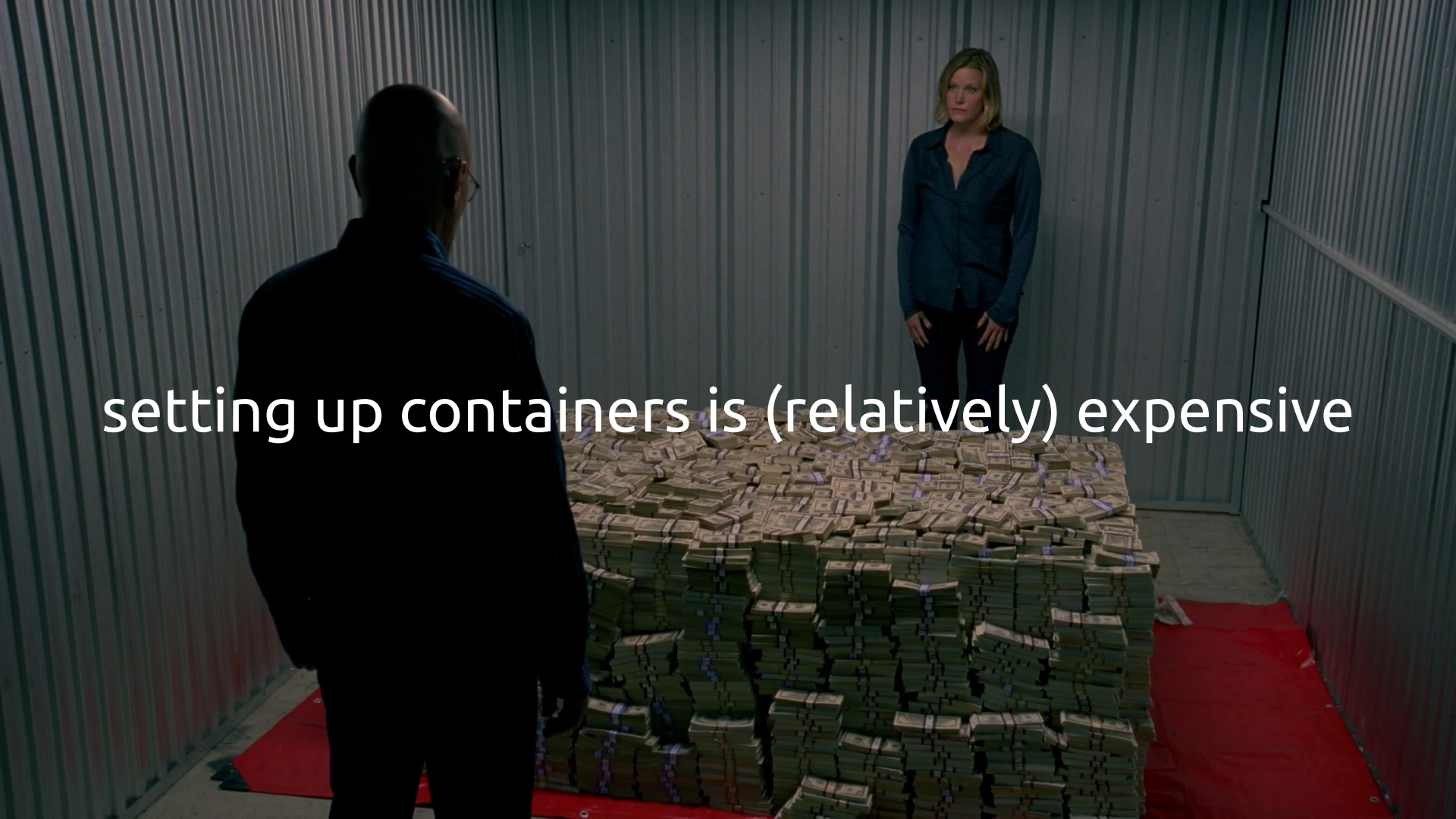
Let's look that up...

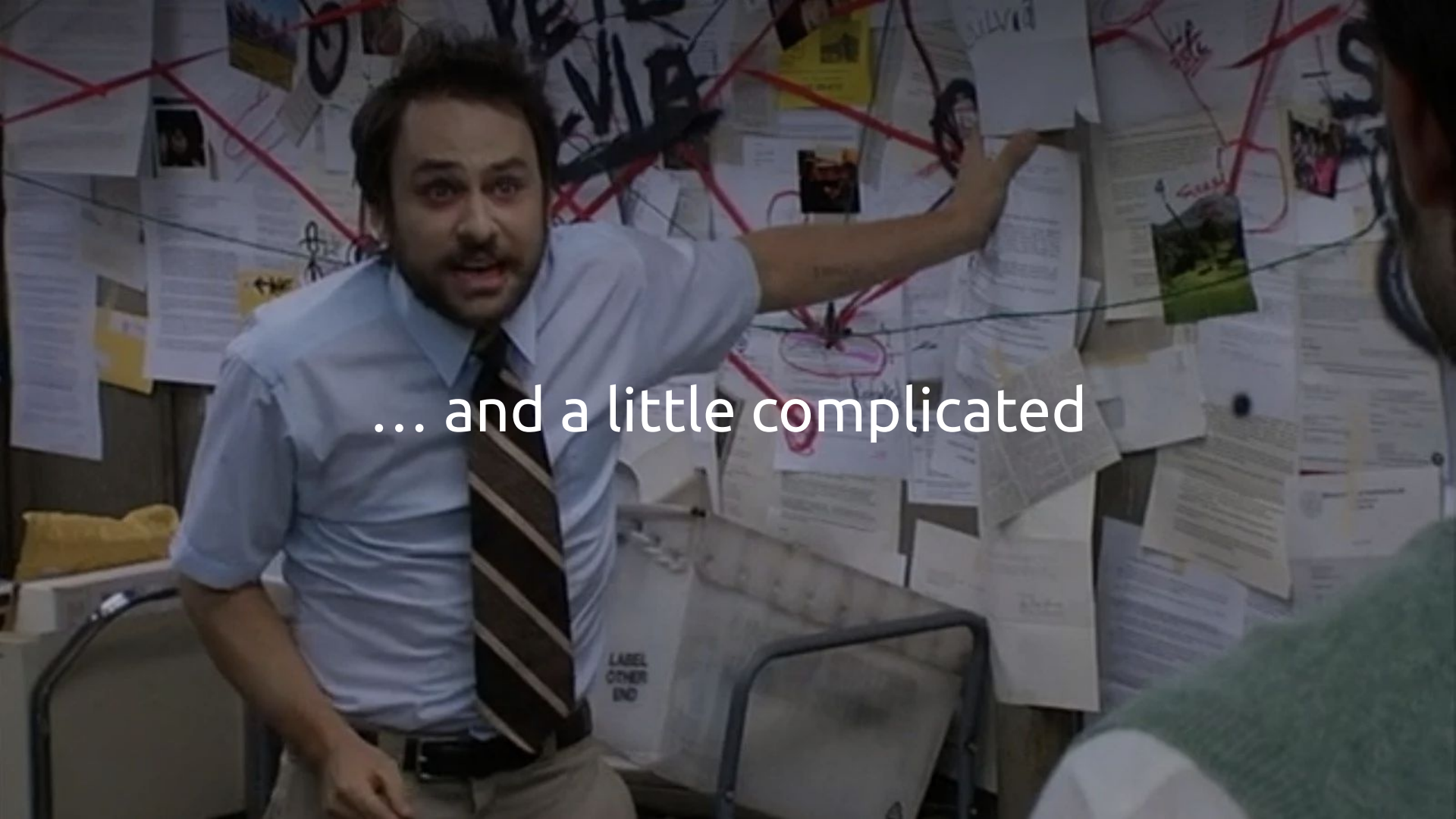
Ah, this points to ../../../foo.


```
/var/www/htdocs/../../../foo
```

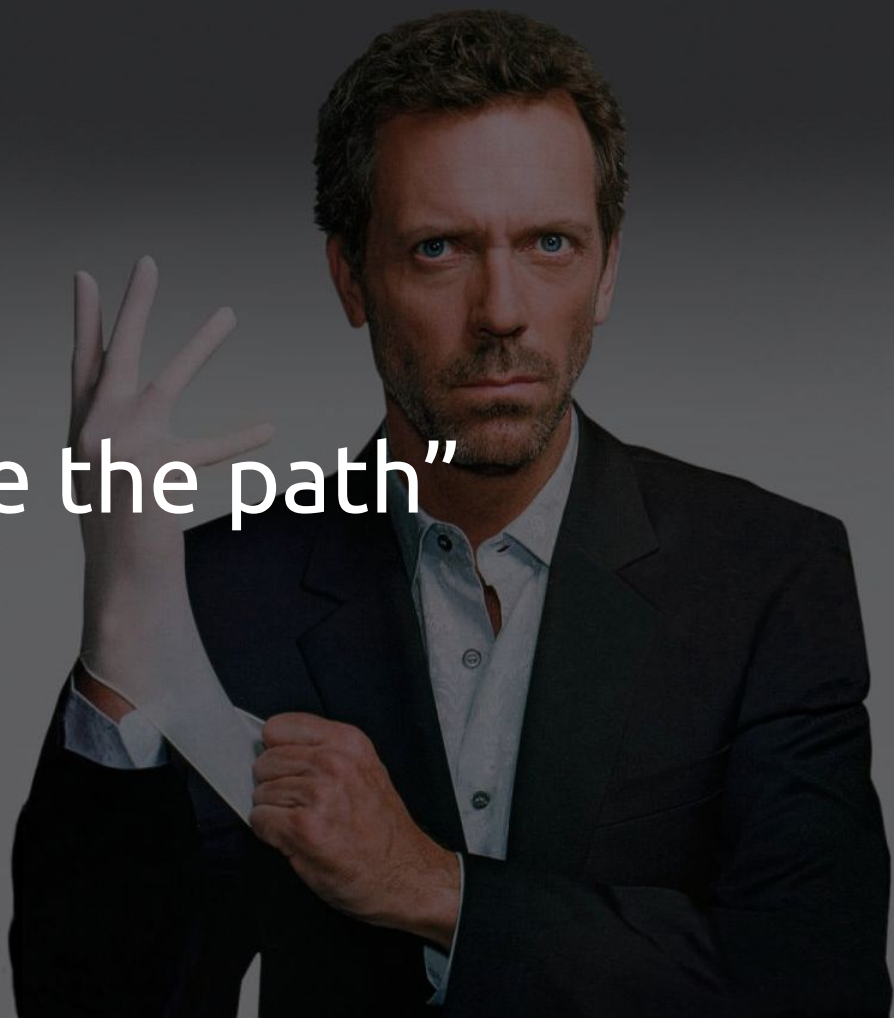
```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            └── files
                └── music.mp3
```

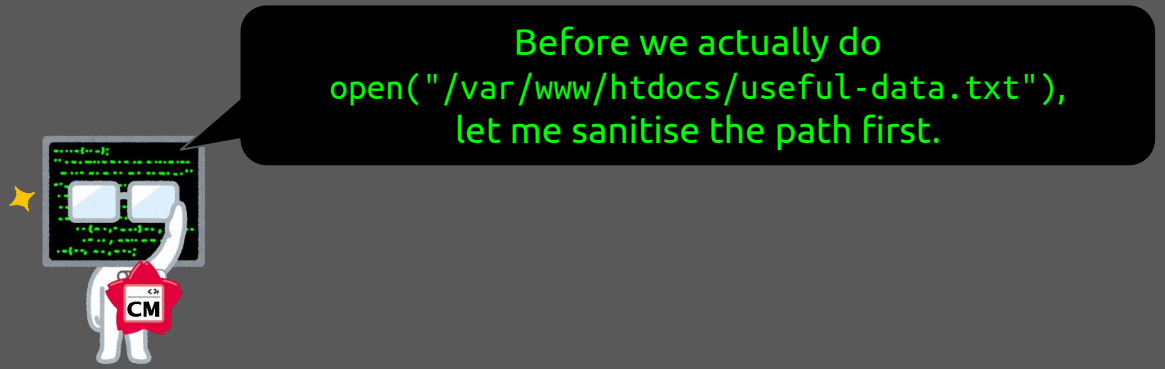

CM


setting up containers is (relatively) expensive


… and a little complicated

“just sanitise the path”




Before we actually do
open("/var/www/htdocs/useful-data.txt"),
let me sanitise the path first.
CM

Before we actually do
`open("/var/www/htdocs/useful-data.txt")`,
let me sanitise the path first.

Ah, `useful-data.txt` was a symlink to `/etc/shadow`,
so I guess we should do
`open("/var/www/htdocs/etc/shadow")`.

Before we actually do `open("/var/www/htdocs/useful-data.txt")`, let me sanitise the path first.

Ah, `useful-data.txt` was a symlink to `/etc/shadow`, so I guess we should do `open("/var/www/htdocs/etc/shadow")`.

Nothing can possibly go wrong, right?

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            ├── dummy-file.txt -> /etc/shadow
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            ├── dummy-file.txt -> /etc/shadow
            └── files
                └── music.mp3
```

You can’t beat me that easily!

Let me sanitise the path first.


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

You can’t beat me that easily!

No symlinks found!

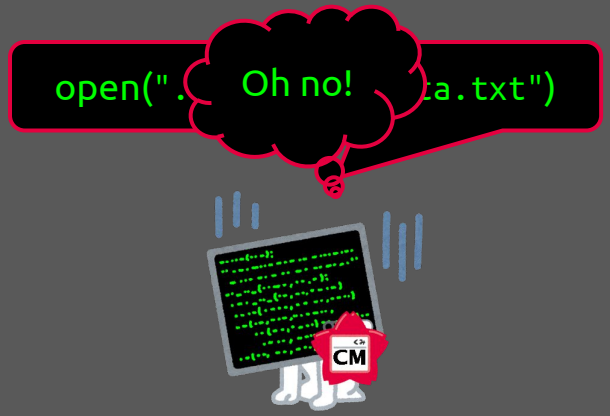

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt
            ├── dummy-file.txt -> /etc/shadow
            └── files
                └── music.mp3
```

You can’t beat me that easily!

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

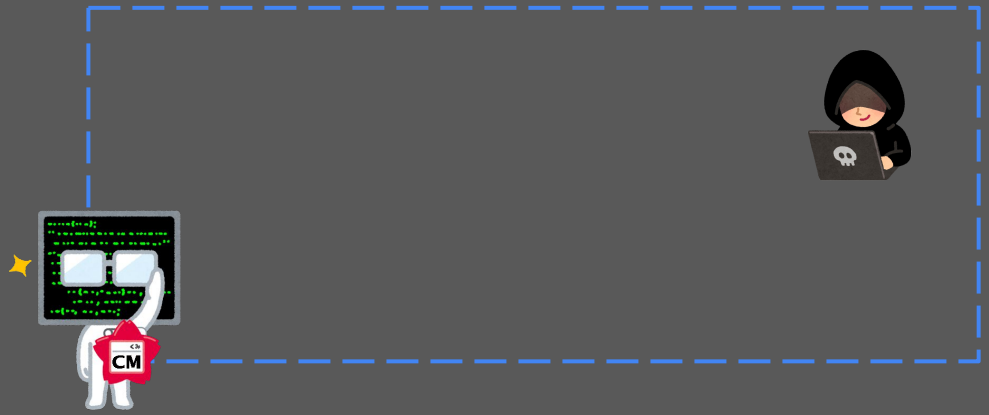
```
open("../useful-data.txt")
```

You can’t beat me that easily!

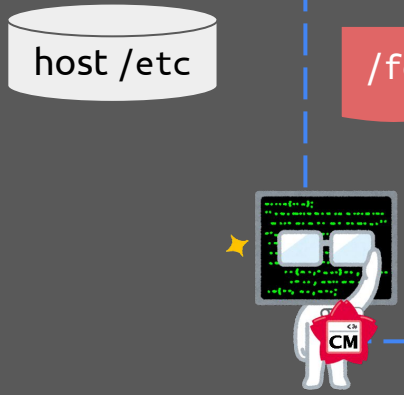



```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

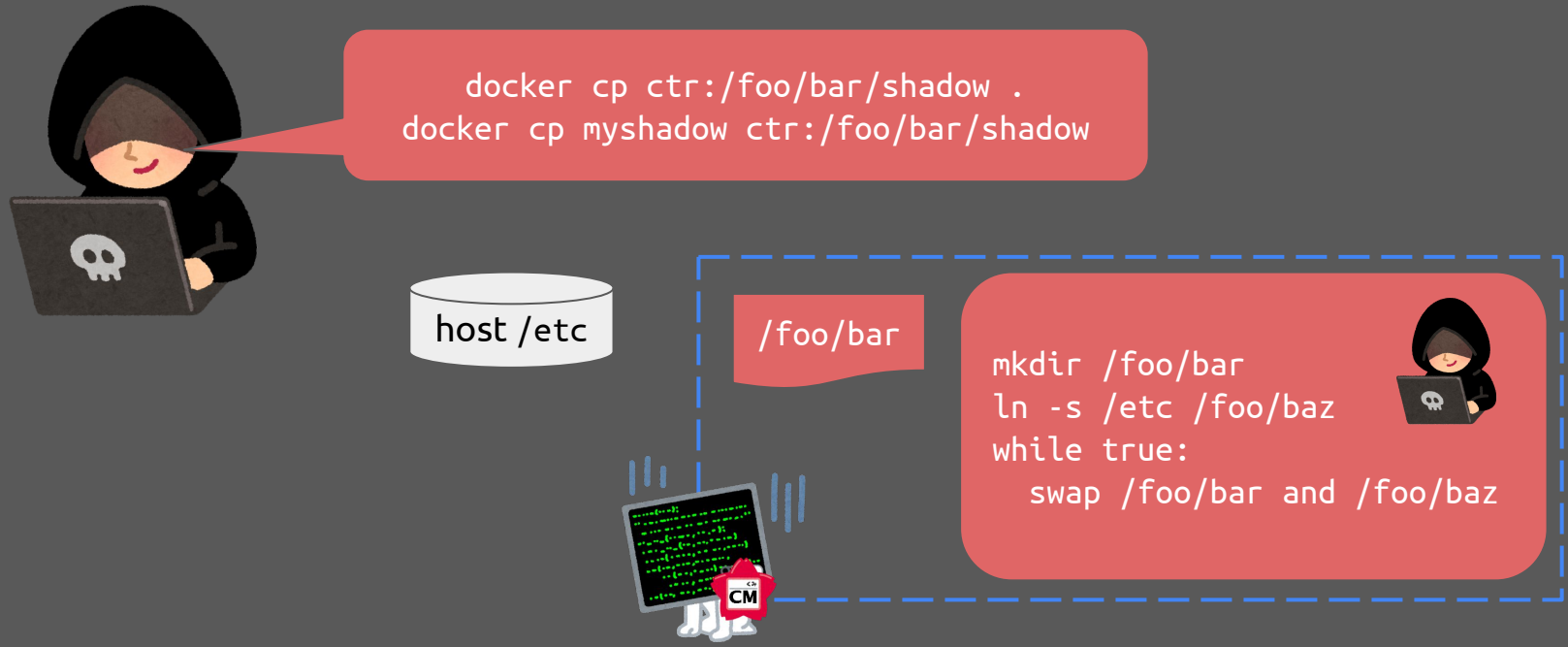
CVE-2018-15664



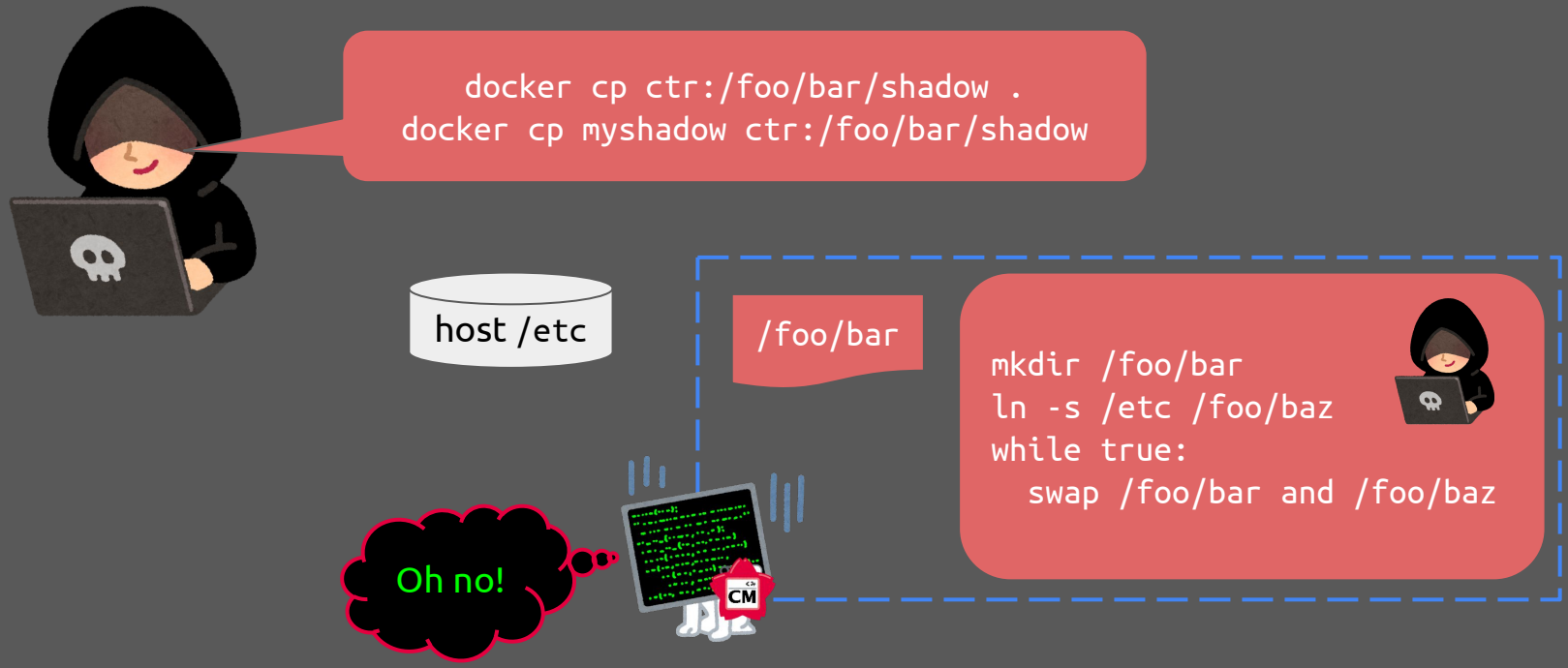
CVE-2018-15664



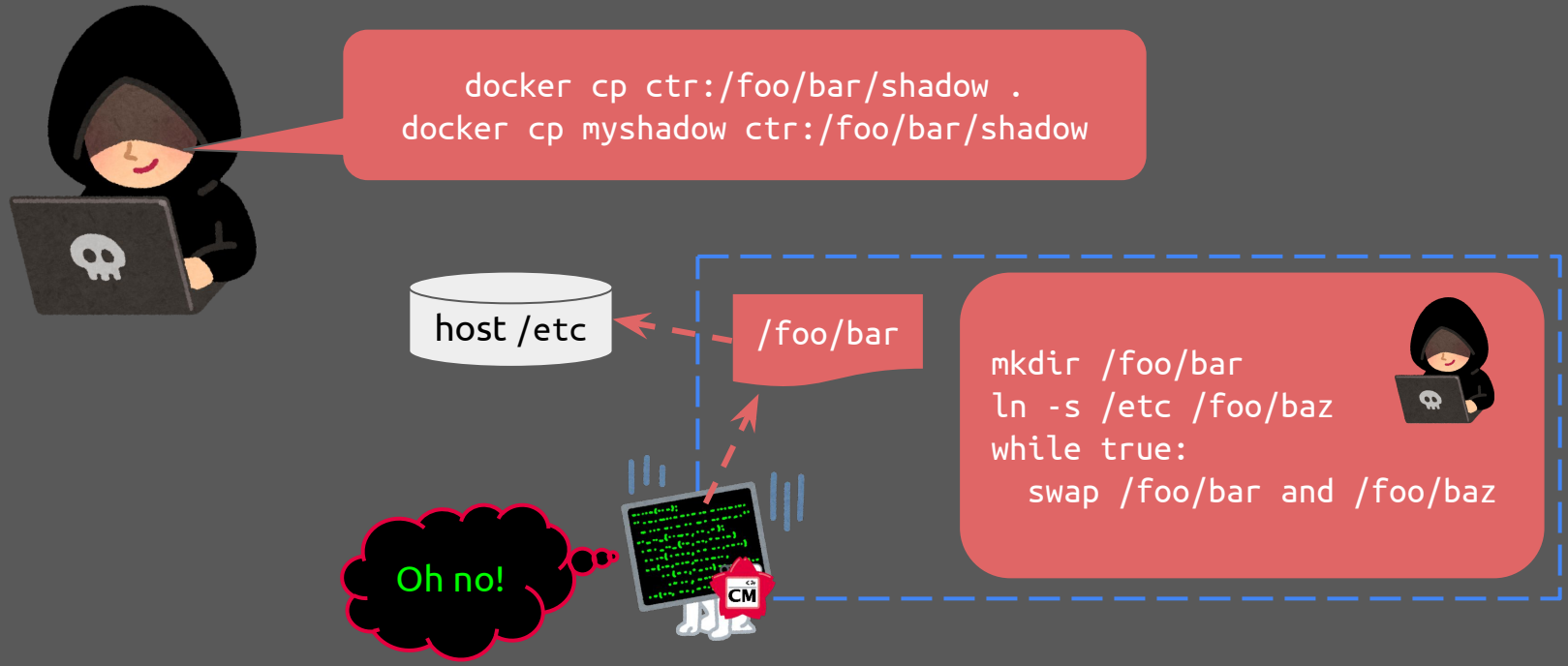
CVE-2018-15664



CVE-2018-15664

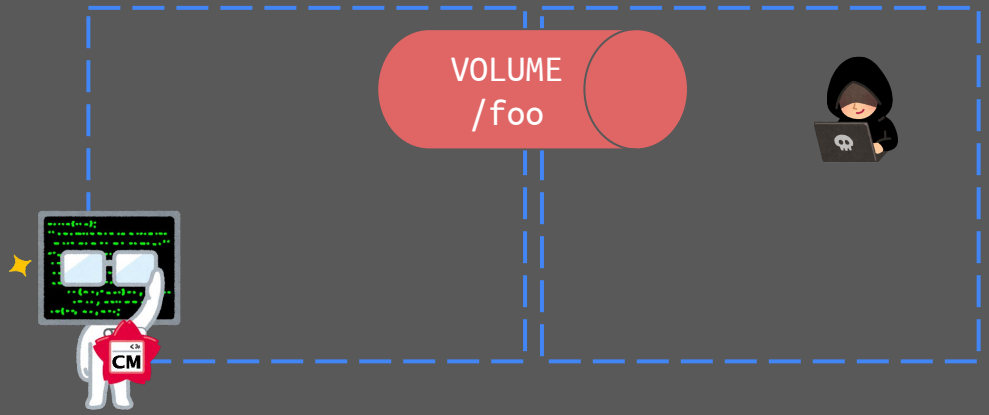


CVE-2018-15664

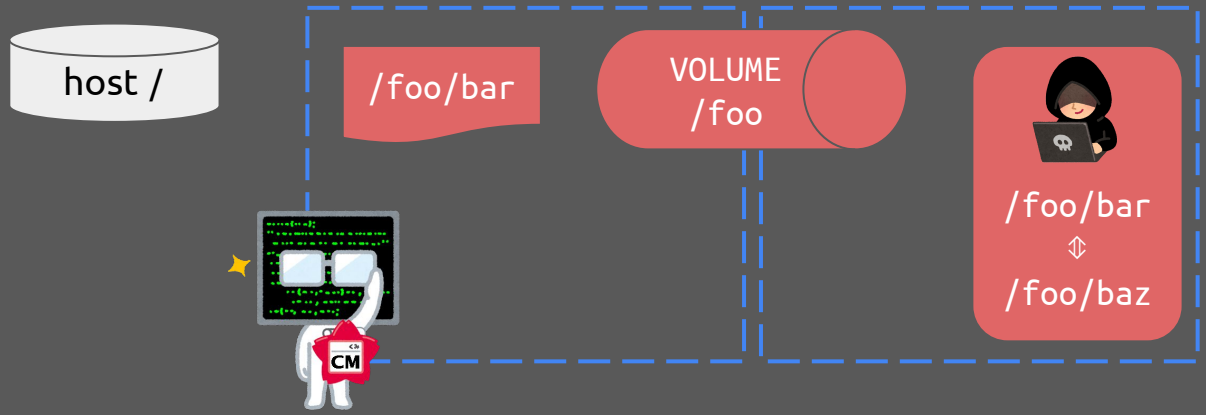



filesystems /
/ a bad time
pick two
MSC

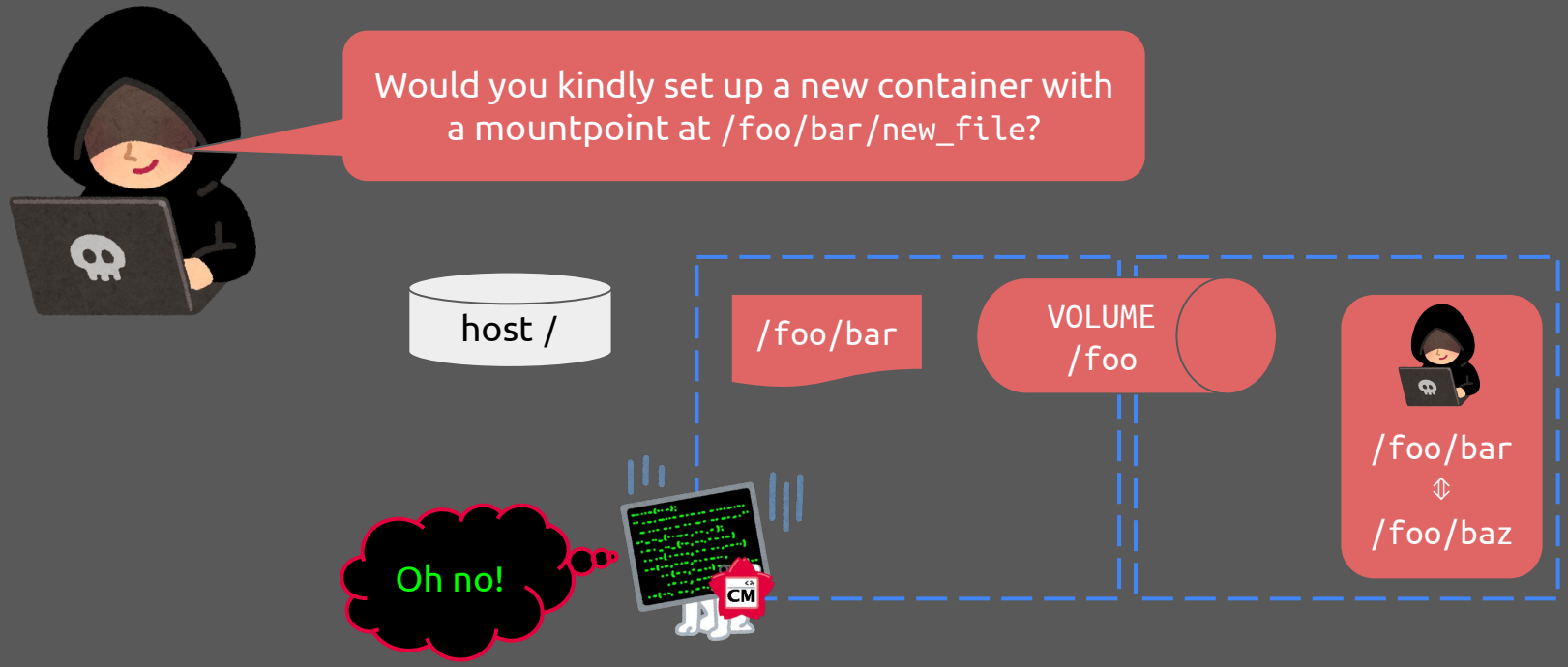
CVE-2024-45310



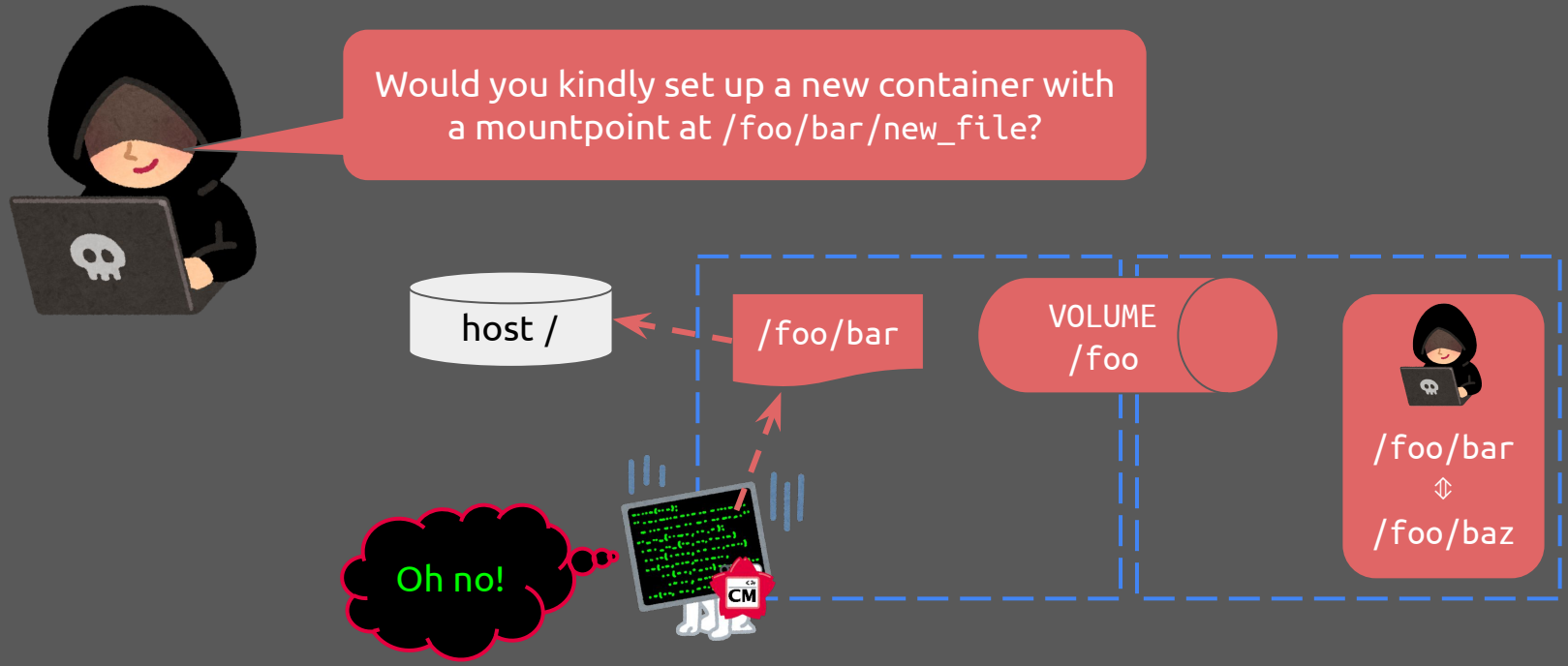
CVE-2024-45310



CVE-2024-45310



CVE-2024-45310

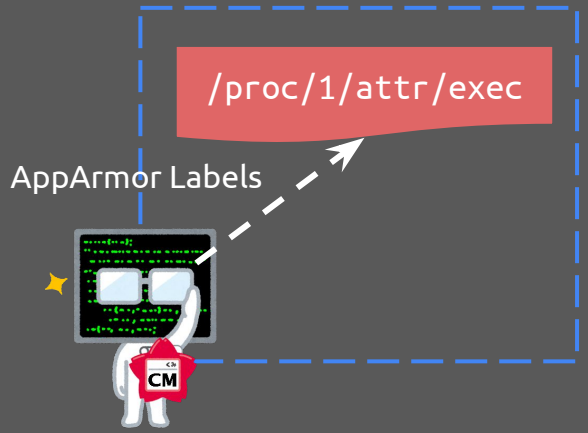


procfs

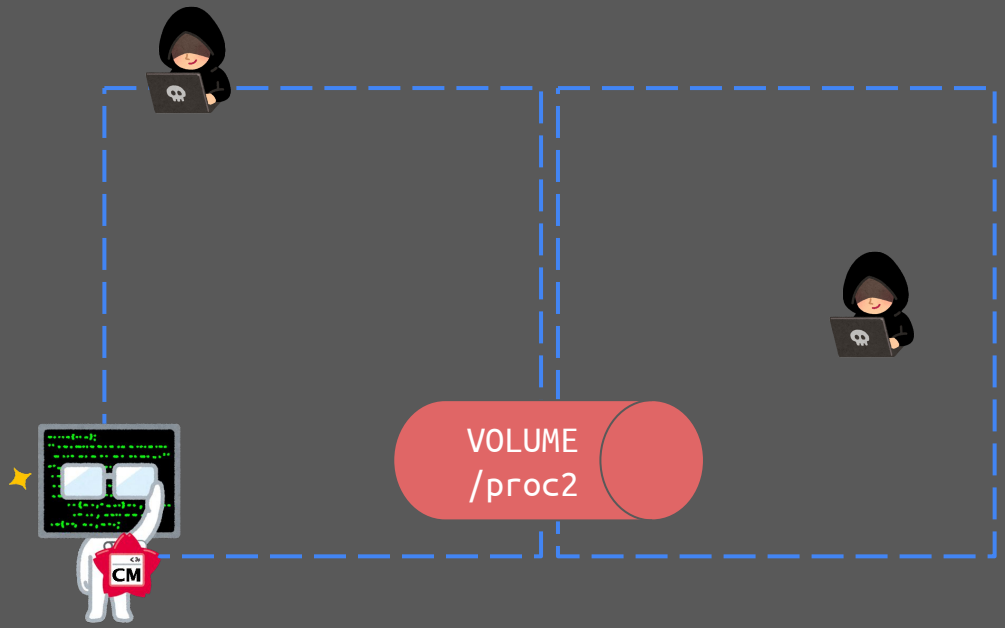
- Pseudofilesystem (more lies!)
- Only Linux API for some key features
- ✨ Magiclinks ✨

```
/proc
├── <pid>
│   ├── attr
│   │   ├── current
│   │   └── exec
│   ├── exe -> ✨/bin/bash✨
│   ├── fd
│   │   ├── 0 -> ✨/dev/pts/1✨
│   │   ├── 1 -> ✨/dev/pts/1✨
│   │   ├── 2 -> ✨/dev/pts/1✨
│   │   └── 3 -> ✨/secrets.txt✨
│   └── mountinfo
├── cpuinfo
└── devices
```

CVE-2019-16884 / CVE-2019-19921

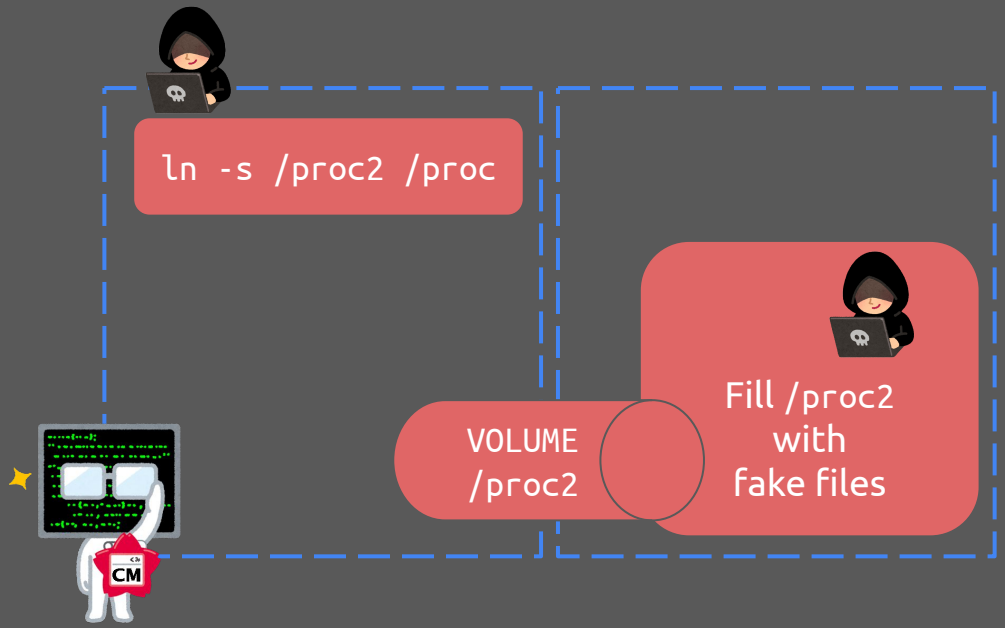


CVE-2019-16884 / CVE-2019-19921



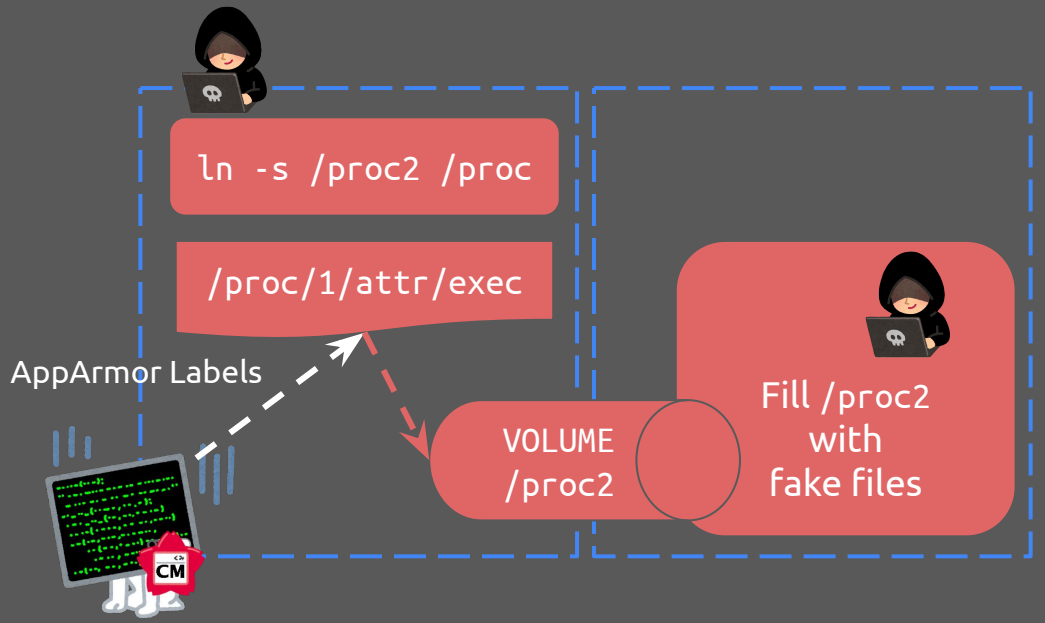
CVE-2019-16884 / CVE-2019-19921

Would you kindly set up a new container with this weird `/proc` configuration?



CVE-2019-16884 / CVE-2019-19921 / CVE-2023-27561

Would you kindly set up a new container with this weird /proc configuration?




foe has appeared!
CHALLENGER APPROACHING

libpathrs

libpathrs

libpathrs

libpathrs

```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```


```
/
├── etc
│   └── shadow
├── tmp
│   └── database.txt
└── var
    └── www
        └── htdocs
            ├── index.html
            ├── upload.php
            ├── useful-data.txt -> /etc/shadow
            ├── dummy-file.txt
            └── files
                └── music.mp3
```

libpathrs

openat2

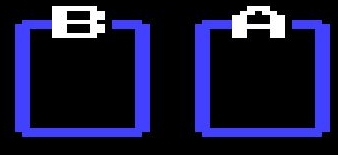
libpathrs

O_PATH

KEEP
CALM
AND
USE
LIBPATHRS


CM


CM




IT'S DANGEROUS TO OPEN PATHS
ALONE! TAKE THIS.