What Userland Utilities Won't Tell You:

Uncovering Hidden Process State in `procfs`

Aivars Kalvāns | aivars.kalvans@gmail.com | https://aivarsk.com

me



» 1999 - Linux (Slackware)
  › C and some C++
» 2001 - Solaris, AIX, HP-UX (PA-RISC, Itanium)
  › PL/SQL, C++, Python, Java...
» 2021 - AWS, Kubernetes, Kafka
» Linux Blue Team



systemd?

DNS?

SYSTEMD-RESOLVED.SERVICE(8) systemd-resolved.serviceSYSTEMD-RESOLVED.SERVICE(8)

NAME

systemd-resolved.service, systemd-resolved - Network Name Resolution manager

SYNOPSIS

systemd-resolved.service

/usr/lib/systemd/systemd-resolved

DESCRIPTION

systemd-resolved is a system service that provides network name resolution to local applications. It implements a caching and validating DNS/DNSSEC stub resolver, as well as an LLMNR and MulticastDNS resolver and responder. Local applications may submit network name resolution requests via three interfaces:

ps

```
» ps aux | grep [s]ystemd-resolved
systemd+  488  0.0  0.0  25600 12800 ?  Ss  Sep09  12:23 /usr/lib/systemd/systemd-resolved
»
```

netstat

```
» netstat -plnt | grep [s]ystemd-resolved
»
```

netstat

```
» netstat -plnt | grep 53
tcp     0     0 127.0.0.54:53     0.0.0.0:*     LISTEN     -
tcp     0     0 127.0.0.53:53     0.0.0.0:*     LISTEN     -
»
```

netstat

```
» netstat -plnt | grep 53
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
»
```

sudo netstat

```
» sudo netstat -plnt | grep [s]ystemd-resolved
»
```

sudo netstat

```
» sudo netstat -plnt | grep 53
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      488/systemd-resolve
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      488/systemd-resolve
»
```

sudo netstat - where is the "d"?

```
» sudo netstat -plnt | grep 53
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      488/systemd-resolve
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      488/systemd-resolve
»
```

top

```
top - 09:00:07 up 28 days,  1:44,  2 users,  load average: 1.37, 1.96, 2.02
Tasks: 519 total,   1 running, 518 sleeping,   0 stopped,   0 zombie
%Cpu(s): 13.7 us,  3.7 sy,  0.0 ni, 82.5 id,  0.1 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  38589.7 total,   4470.9 free,  27949.8 used,   9376.6 buff/cache
MiB Swap:   8192.0 total,    797.0 free,   7395.0 used.  10639.9 avail Mem
add filter #1 (ignoring case) as: [!]FLD?VAL PID=488
    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
1451682 aivarsk   20   0 1449.3g 485292 180352 S  37.9   1.2     6d+4h chrome
1063130 aivarsk   20   0 1448.1g 203360 156528 S  22.3   0.5   0:03.28 chrome
   1887 root      20   0 3520864  12520   5344 S   9.5   0.0 156:33.11 confighandler
3982033 aivarsk   20   0 5155424 198168  50044 S   5.0   0.5 360:34.38 dropbox
```

top - where is the "d"?

```
top - 09:00:29 up 28 days,  1:45,  2 users,  load average: 2.07, 2.08, 2.06
Tasks: 521 total,   2 running, 519 sleeping,   0 stopped,   0 zombie
%Cpu(s): 14.4 us,  4.1 sy,  0.0 ni, 81.4 id,  0.1 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  38589.7 total,   4396.4 free,  28024.2 used,   9377.5 buff/cache
MiB Swap:   8192.0 total,    797.0 free,   7395.0 used.  10565.6 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  14883 aivarsk   20   0 1450.0g 459340 155388 S   0.3   1.2  47:48.08 chrome
    488 systemd+  20   0   25600  12800  10404 S   0.0   0.0  12:23.90 systemd-resolve
```

Which one?

- `/usr/lib/systemd/systemd-resolved`
- `systemd-resolve`
- `systemd-resolve`**`d`**

UNIX 8th Edition, 1984

Processes as Files

T. J. Killian

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

We describe a new file system, **/proc**, each member of which, **/proc/***nnnnn*, corresponds to the address space of the running process whose pid is *nnnnn*. Access to these files is restricted, via the normal file protection mechanism, to the process owner. *Lseek*(2), *read*(2), and *write*(2), allow inspection and modification of the process' image. Other services are available via *ioctl*(2), including stop/go on demand, selective intercepting of signals, and the ability to obtain an open file descriptor for the process' text file. The techni

The discovery process

```
» strace -e file netstat -plnt 2>&1 | grep '"/proc/'
openat(AT_FDCWD, "/proc/filesystems", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/proc/net/tcp", O_RDONLY) = 3
openat(AT_FDCWD, "/proc/net/tcp6", O_RDONLY) = 3
...
»
```

https://linux.die.net/man/5/proc

/proc/pid/comm - command name

```
» cat /proc/488/comm
systemd-resolve
»
```

/proc/pid/stat - status information

```
» cat /proc/488/stat
488 (systemd-resolve) S 1 488 488 0 -1 4194560 5196 93 43 0 47602 28154 0 0 20 0 1 0 396
↪ 26214400 3364 18446744073709551615 1 1 0 0 0 0 18947 4096 0 0 0 0 17 4 0 0 0 0 0 0 0 0
↪ 0 0 0 0 0
»
```

/proc/pid/status - memory usage and status information

```
» cat /proc/488/status | head -3
Name:   systemd-resolve
Umask:  0022
State:  S (sleeping)
»
```

/proc/pid/cmdline - command line

```
» cat /proc/488/cmdline | tr '\0' '\n'
/usr/lib/systemd/systemd-resolved
»
```

Who stole "d"?

linux/sched.h:

```
/*
 * Define the task command name length as enum, then it can be visible to
 * BPF programs.
 */
enum {
        TASK_COMM_LEN = 16,
};
```

Summary

- » top, netstat, ...
  - › /proc/pid/comm, /proc/pid/stat, /proc/pid/status
- » ps, ...
  - › /proc/pid/cmdline

Right?

- top, netstat, ...
  - /proc/pid/comm, /proc/pid/stat, /proc/pid/status
- ps, ...
  - /proc/pid/cmdline

Ackchyuually...

```
» ps p 3
    PID TTY      STAT   TIME COMMAND
      3 ?        S      0:00 [pool_workqueue_release]
»
```

Ackchyuually...

```
» ps p 3
    PID TTY      STAT   TIME COMMAND
      3 ?        S      0:00 [pool_workqueue_release]
» cat /proc/3/cmdline | tr '\0' '\n'
»
```

Ackchyuually...

```
» ps p 3
    PID TTY      STAT   TIME COMMAND
      3 ?        S      0:00 [pool_workqueue_release]
» cat /proc/3/cmdline | tr '\0' '\n'
» sudo cat /proc/3/cmdline | tr '\0' '\n'
»
```

Ackchyuually...

```
» ps p 3
    PID TTY      STAT   TIME COMMAND
      3 ?        S      0:00 [pool_workqueue_release]
» cat /proc/3/cmdline | tr '\0' '\n'
» sudo cat /proc/3/cmdline | tr '\0' '\n'
» cat /proc/3/comm
pool_workqueue_release
»
```

Kthread - kernel thread flag, 1 is yes, 0 is no

```
» cat /proc/3/status | grep Kthread
Kthread:        1
»
```

ps and kernel threads

» show `/proc/pid/cmdline`

» when empty, show `/proc/pid/comm`

» inside square brackets []

› that's how you know it's a kernel thread

» and, BTW, no 15 char limit

› pool_workqueue_release is 22 chars + zero

netstat, lsof, fuser, ... ?

/proc/pid/fd/ - file descriptors

```
» ls -l /proc/488/fd/
ls: cannot open directory '/proc/488/fd/': Permission denied
»
```

/proc/pid/fd/ - file descriptors

```
» ls -l /proc/488/fd/
ls: cannot open directory '/proc/488/fd/': Permission denied
» sudo ls -l /proc/488/fd/
total 0
lr-x------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 0 -> /dev/null
lrwx------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 1 -> 'socket:[10261]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 10 -> 'anon_inode:[timerfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 11 -> 'anon_inode:[timerfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 12 -> 'anon_inode:[pidfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 13 ->
↪ /sys/fs/cgroup/system.slice/systemd-resolved.service/memory.pressure
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 14 -> 'socket:[9686]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 15 -> 'socket:[9687]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 16 -> 'socket:[9688]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 17 -> 'socket:[9689]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 18 -> 'socket:[9690]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 19 -> 'socket:[9691]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 2 -> 'socket:[10261]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 20 -> 'socket:[14953]'
...
»
```

/proc/pid/fd/ - file descriptors

```
» cat /proc/2578925/comm
precached
» sudo ls -l /proc/2578925/fd/
total 0
lrwx------ 1 root root 64 Oct 13 10:55 0 -> /dev/pts/18
lrwx------ 1 root root 64 Oct 13 10:55 1 -> /dev/pts/18
lrwx------ 1 root root 64 Oct 13 10:55 2 -> /dev/pts/18
lr-x------ 1 root root 64 Oct 13 10:55 3 -> /etc/shadow
»
```

/proc/pid/fd/ - file descriptors

```
» ls -l /proc/488/fd/
ls: cannot open directory '/proc/488/fd/': Permission denied
» sudo ls -l /proc/488/fd/
total 0
lr-x------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 0 -> /dev/null
lrwx------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 1 -> 'socket:[10261]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 10 -> 'anon_inode:[timerfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 11 -> 'anon_inode:[timerfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 12 -> 'anon_inode:[pidfd]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 13 ->
↪ /sys/fs/cgroup/system.slice/systemd-resolved.service/memory.pressure
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 14 -> 'socket:[9686]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 15 -> 'socket:[9687]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 16 -> 'socket:[9688]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 17 -> 'socket:[9689]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 18 -> 'socket:[9690]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 19 -> 'socket:[9691]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Sep  9 07:15 2 -> 'socket:[10261]'
lrwx------ 1 systemd-resolve systemd-resolve 64 Oct 10 01:16 20 -> 'socket:[14953]'
...
»
```

/proc/net/tcp - a dump of the TCP socket table

```
» cat /proc/net/tcp | head -1
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
↪ timeout inode
» cat /proc/net/tcp | grep -E "10261|9686|9687|9688|9689|9690|9691|10261|14953"
  10: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9689 1 0000000000000000 100 0 0 10 5
  11: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9687 1 0000000000000000 100 0 0 10 5
»
```

0035

/proc/net/tcp - a dump of the TCP socket table

```
» cat /proc/net/tcp | head -1
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
↪ timeout inode
» cat /proc/net/tcp | grep -E "10261|9686|9687|9688|9689|9690|9691|10261|14953"
  10: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9689 1 0000000000000000 100 0 0 10 5
  11: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9687 1 0000000000000000 100 0 0 10 5
»
```

LISTEN

/proc/net/tcp - a dump of the TCP socket table

```
» cat /proc/net/tcp | head -1
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
↪ timeout inode
» cat /proc/net/tcp | grep -E "10261|9686|9687|9688|9689|9690|9691|10261|14953"
  10: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9689 1 0000000000000000 100 0 0 10 5
  11: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9687 1 0000000000000000 100 0 0 10 5
»
```

LISTEN
PORT 53

/proc/net/tcp - a dump of the TCP socket table

```
» cat /proc/net/tcp | head -1
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
↪ timeout inode
» cat /proc/net/tcp | grep -E "10261|9686|9687|9688|9689|9690|9691|10261|14953"
  10: 3600007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9689 1 0000000000000000 100 0 0 10 5
  11: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   991
↪ 0 9687 1 0000000000000000 100 0 0 10 5
»
```

LISTEN

PORT 53

IP 127.0.0.54, 127.0.0.53

pstree

Process tree

```
» pstree -spc 488
systemd(1)───systemd-resolve(488)
»
```

Process tree

```
» pstree -spc 488
systemd(1)───systemd-resolve(488)
» pstree -spc 2255341
systemd(1)───systemd(2357)───zellij(520153)───bash(2255281)───sleep(2255341)
»
```

Process tree

```
» pstree -spc 488
systemd(1)───systemd-resolve(488)
» pstree -spc 2255341
systemd(1)───systemd(2357)───zellij(520153)───bash(2255281)───sleep(2255341)
» pstree -spc 2256468
systemd(1)───systemd(2357)───notabackdoor(2256468)
»
```

PPid - process id of the parent process

```
» cat /proc/488/status | grep PPid
PPid:   1
»
```

Orphaned process adopted by PID=1 or child subreaper

```
» cat noparent.c
#include <unistd.h>

int main() {
     if (fork() == 0) {
          return sleep(2147447412);
     }
     return 0;
}
» gcc -Wall -o notabackdoor noparent.c
»
```

/proc/pid/cgroup - control group

```
» cat /proc/2256468/cgroup
0::/user.slice/user-1000.slice/user@1000.service/app.slice/app-gnome-Alacritty-520116.scop
↪ e
»
```

/proc/pid/cgroup - control group

```
» cat /proc/2256468/cgroup
0::/user.slice/user-1000.slice/user@1000.service/app.slice/app-gnome-Alacritty-520116.scop
↪ e
» id -nu 1000
aivarsk
»
```

/proc/pid/cgroup - control group

```
» cat /proc/2256468/cgroup
0::/user.slice/user-1000.slice/user@1000.service/app.slice/app-gnome-Alacritty-520116.scop
↪ e
» id -nu 1000
aivarsk
» ps up 520116
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk   520116  0.1  0.0 957736 24444 ?        Sl   Sep13  50:29 /usr/bin/alacritty
»
```

/proc/pid/environ - initial environment

```
» cat /proc/2256468/environ | tr '\0' '\n'
SESSION_MANAGER=local/t480s:@/tmp/.ICE-unix/2698,unix/t480s:/tmp/.ICE-unix/2698
JAVA_HOME=/home/aivarsk/.local/share/mise/installs/java/25.0.1
PWD=/home/aivarsk/procfs
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=aivarsk
ZELLIJ_PANE_ID=29
XDG_SESSION_TYPE=wayland
HOME=/home/aivarsk
USERNAME=aivarsk
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=ubuntu:GNOME
MEMORY_PRESSURE_WATCH=/sys/fs/cgroup/user.slice/user-1000.slice/user@1000.service/session.
↪ slice/org.gnome.Shell@wayland.service/memory.pressure
_=./notabackdoor
...
»
```

Very legitimate process, I promise.

Faking command line from the outside

```
» cat badexec.c
#include <unistd.h>

int main() {
     char *path = "/usr/bin/sleep";
     char *argv[] = {"[commouflage]", "inf", NULL};
     return execv(path, argv);
}
» gcc -Wall -o badexec badexec.c
»
```

Faking command line from the outside

```
» cat badexec.c
#include <unistd.h>

int main() {
     char *path = "/usr/bin/sleep";
     char *argv[] = {"[commouflage]", "inf", NULL};
     return execv(path, argv);
}
» gcc -Wall -o badexec badexec.c
» ./badexec &
[1] 1278141
»
```

Faking command line from the outside

```
» cat /proc/1278141/cmdline | tr '\0' '\n'
[commouflage]
inf
»
```

Faking command line from the outside

```
» cat /proc/1278141/cmdline | tr '\0' '\n'
[commouflage]
inf
» ps p 1278141
    PID TTY      STAT   TIME COMMAND
1278141 pts/44   S      0:00 [commouflage] inf
»
```

Faking command line from the inside

```
» cat badargv0.c
#include <string.h>
#include <unistd.h>

int main(int argc, char *argv[]) {
     memset(argv[0], ' ', strlen(argv[0]));
     strcpy(argv[0], "[commouflage]");
     return sleep(2147447412);
}
» gcc -Wall -o badargv0 badargv0.c
»
```

Faking command line from the inside

```
» cat badargv0.c
#include <string.h>
#include <unistd.h>

int main(int argc, char *argv[]) {
     memset(argv[0], ' ', strlen(argv[0]));
     strcpy(argv[0], "[commouflage]");
     return sleep(2147447412);
}
» gcc -Wall -o badargv0 badargv0.c
» ./badargv0 &
[1] 1279340
»
```

Faking command line from the inside

```
» cat /proc/1279340/cmdline | tr '\0' '\n'
[commouflage]
»
```

Faking command line from the inside

```
» cat /proc/1279340/cmdline | tr '\0' '\n'
[commouflage]
» ps p 1279340
    PID TTY      STAT   TIME COMMAND
1279340 pts/44   S      0:00 [commouflage]
»
```

We can't trust the command line.

Can we trust the command name?

Faking command name from the outside

```
» ln -s `which sleep` decepticon
» ./decepticon inf &
[1] 1283175
»
```

Faking command name from the outside

```
» cat /proc/1283175/comm
decepticon
»
```

Faking command name from the outside

```
» cat /proc/1283175/comm
decepticon
» cat /proc/1283175/cmdline | tr '\0' '\n'
./decepticon
inf
»
```

Faking command name from the inside

```
» cat badcomm.c
#include <sys/prctl.h>
#include <unistd.h>

int main() {
     prctl(PR_SET_NAME, "decepticon");
     return sleep(2147447412);
}
» gcc -Wall -o badcomm badcomm.c
» ./badcomm &
[1] 1284448
»
```

Faking command name from the inside

```
» cat /proc/1284448/comm
decepticon
»
```

Faking command name from the inside

```
» cat /proc/1284448/comm
decepticon
» cat /proc/1284448/cmdline | tr '\0' '\n'
./badcomm
»
```

Faking is good, sometimes

- multi-call binaries
  - busybox, ...
- versioned binaries

```
» which python3
/usr/bin/python3
» readlink /usr/bin/python3
python3.13
```

/proc/pid/exe - symbolic link to program pathname

```
» readlink /proc/488/exe
»
```

/proc/pid/exe - symbolic link to program pathname

```
» readlink /proc/488/exe
» sudo readlink /proc/488/exe
/usr/lib/systemd/systemd-resolved
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
» rm ./badcomm
»
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
» rm ./badcomm
»
» readlink /proc/1289962/exe
/home/aivarsk/procfs/badcomm (deleted)
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
» rm ./badcomm
»
» readlink /proc/1289962/exe
/home/aivarsk/procfs/badcomm (deleted)
» ls -l /home/aivarsk/procfs/badcomm
"/home/aivarsk/procfs/badcomm": No such file or directory (os error 2)
»
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
» rm ./badcomm
»
» readlink /proc/1289962/exe
/home/aivarsk/procfs/badcomm (deleted)
» ls -l /home/aivarsk/procfs/badcomm
"/home/aivarsk/procfs/badcomm": No such file or directory (os error 2)
»
» cat /proc/1289962/exe > badcomm.restored
»
```

Hiding from /proc/pid/exe

```
» ./badcomm &
[1] 1289962
» md5sum ./badcomm
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm
» rm ./badcomm
»
» readlink /proc/1289962/exe
/home/aivarsk/procfs/badcomm (deleted)
» ls -l /home/aivarsk/procfs/badcomm
"/home/aivarsk/procfs/badcomm": No such file or directory (os error 2)
»
» cat /proc/1289962/exe > badcomm.restored
» md5sum ./badcomm.restored
9e8e6d758df25f9cbb571bb35a9e9641  ./badcomm.restored
»
```

Hiding from /proc/pid/exe in memory

```
» cat memfd.c
#define _GNU_SOURCE
#include <fcntl.h>
#include <sys/mman.h>
#include <unistd.h>

int main() {
     int src = open("/usr/bin/sleep", 0);
     int mem = memfd_create("x", 1);

     char buf[4096];
     int n;
     while ((n = read(src, buf, 4096)) > 0)
          write(mem, buf, n);

     char *argv[] = {"phony", "inf", NULL};
     char *envp[] = {NULL};
     fexecve(mem, argv, envp);
}
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
» ./memfd &
[1] 1294565
»
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
» ./memfd &
[1] 1294565
»
» cat /proc/1294565/comm
memfd:x
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
» ./memfd &
[1] 1294565
»
» cat /proc/1294565/comm
memfd:x
» readlink /proc/1294565/exe
/memfd:x (deleted)
»
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
» ./memfd &
[1] 1294565
»
» cat /proc/1294565/comm
memfd:x
» readlink /proc/1294565/exe
/memfd:x (deleted)
»
» cat /proc/1294565/exe > memfd.restored
»
```

Hiding from /proc/pid/exe in memory

```
» gcc -Wall -o memfd memfd.c
» ./memfd &
[1] 1294565
»
» cat /proc/1294565/comm
memfd:x
» readlink /proc/1294565/exe
/memfd:x (deleted)
»
» cat /proc/1294565/exe > memfd.restored
» md5sum /usr/bin/sleep memfd.restored
2b8ca12a8081d85a6dd75235cde8b8db  /usr/bin/sleep
2b8ca12a8081d85a6dd75235cde8b8db  memfd.restored
»
```

Can we trust the /proc/pid/exe then?

The binary and libraries

```
» cd / && { echo /usr/bin/sleep; ldd /usr/bin/sleep | grep -oE '/[^ ]+'; } |
while read -r f; do
  f=$(readlink -f "$f")
  p=$(dpkg -S "$f" | head -1 | sed 's/: .*//')
  grep -F " ${f#/}" /var/lib/dpkg/info/"$p".md5sums 2>/dev/null
done | md5sum -c -
usr/bin/sleep: OK
usr/lib/x86_64-linux-gnu/libc.so.6: OK
usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2: OK
```

/proc/pid/mem - memory

```
» cat /proc/488/mem
cat: /proc/488/mem: Permission denied
»
```

/proc/pid/mem - memory

```
» cat /proc/488/mem
cat: /proc/488/mem: Permission denied
» sudo cat /proc/488/mem
cat: /proc/488/mem: Input/output error
»
```

/proc/pid/maps - mapped memory regions

```
» sudo cat /proc/488/maps | head
6554af3a0000-6554af3ae000 r--p 00000000 103:06 13243764
↪ /usr/lib/systemd/systemd-resolved
6554af3ae000-6554af41e000 r-xp 0000e000 103:06 13243764
↪ /usr/lib/systemd/systemd-resolved
6554af41e000-6554af439000 r--p 0007e000 103:06 13243764
↪ /usr/lib/systemd/systemd-resolved
6554af439000-6554af43e000 r--p 00098000 103:06 13243764
↪ /usr/lib/systemd/systemd-resolved
6554af43e000-6554af43f000 rw-p 0009d000 103:06 13243764
↪ /usr/lib/systemd/systemd-resolved
6554cb98d000-6554cbd6e000 rw-p 00000000 00:00 0           [heap]
73426cf13000-73426cf54000 rw-p 00000000 00:00 0
73426cf54000-73426cf66000 r--p 00000000 103:06 13246167
↪ /usr/lib/x86_64-linux-gnu/libunistring.so.5.2.0
...
»
```

/proc/pid/map_files/ - memory-mapped files

```
» sudo ls -l /proc/488/map_files
total 0
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 6554af3a0000-6554af3ae000 ->
↪ /usr/lib/systemd/systemd-resolved
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 6554af3ae000-6554af41e000 ->
↪ /usr/lib/systemd/systemd-resolved
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 6554af41e000-6554af439000 ->
↪ /usr/lib/systemd/systemd-resolved
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 6554af439000-6554af43e000 ->
↪ /usr/lib/systemd/systemd-resolved
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 6554af43e000-6554af43f000 ->
↪ /usr/lib/systemd/systemd-resolved
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 11 18:43 73426cf54000-73426cf66000 ->
↪ /usr/lib/x86_64-linux-gnu/libunistring.so.5.2.0
lr-------- 1 systemd-resolve systemd-resolve 64 Oct 13 13:30 73426cf66000-73426cfb1000 ->
↪ /usr/lib/x86_64-linux-gnu/libunistring.so.5.2.0
...
»
```

memgrep helper

```
» memgrep() { while read -r a x; do [[ $x == r* ]] && sudo dd if=/proc/$1/mem bs=1M
↪ iflag=skip_bytes,count_bytes skip=$((16#${a%-*})) count=$((16#${a#*-}-16#${a%-*}))
↪ 2>/dev/null; done < <(sudo cat /proc/$1/maps) | strings | grep -ai "$2"; }
»
```

sleep or backdoor?

```
» readlink /proc/1872364/exe
/usr/bin/sleep
»
```

sleep or backdoor?

```
» readlink /proc/1872364/exe
/usr/bin/sleep
» memgrep 1872364 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
»
```

/etc/ld.so.preload

```
» cat /etc/ld.so.preload
/home/aivarsk/hehe/dlpause.so
»
```

/etc/ld.so.preload

```
» cat /etc/ld.so.preload
/home/aivarsk/hehe/dlpause.so
» cat /proc/1872364/maps | grep hehe
7be99b67a000-7be99b67b000 r--p 00000000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
7be99b67b000-7be99b67c000 r-xp 00001000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
7be99b67c000-7be99b67d000 r--p 00002000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
7be99b67d000-7be99b67e000 r--p 00002000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
7be99b67e000-7be99b67f000 rw-p 00003000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
»
```

sleep or backdoor?

```
» readlink /proc/1875587/exe
/usr/bin/sleep
»
```

sleep or backdoor?

```
» readlink /proc/1875587/exe
/usr/bin/sleep
» memgrep 1875587 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
»
```

sleep or backdoor?

```
» readlink /proc/1875587/exe
/usr/bin/sleep
» memgrep 1875587 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
»
```

sleep or backdoor?

```
» readlink /proc/1875587/exe
/usr/bin/sleep
» memgrep 1875587 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
» cat /proc/1875587/maps | grep hehe
71063460d000-71063460e000 r--p 00000000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
71063460e000-71063460f000 r-xp 00001000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
71063460f000-710634610000 r--p 00002000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
710634610000-710634611000 r--p 00002000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
710634611000-710634612000 rw-p 00003000 103:06 6720024
↪ /home/aivarsk/hehe/dlpause.so
»
```

LD_PRELOAD

```
» cat /proc/1875587/environ | tr '\0' '\n' | grep LD_PRELOAD
LD_PRELOAD=./dlpause.so
»
```

/proc/pid/cwd - link to current working directory

```
» readlink /proc/1875587/cwd
/home/aivarsk/hehe
»
```

Preloaded library

```
» cat dlpause.c
#define _GNU_SOURCE
#include <stdio.h>
#include <dlfcn.h>

const char msg[] = "Backdoor? I prefer the term 'surprise entrance'.";
int pause(void) {
    static int (*r)(void);
    if (!r) r = dlsym(RTLD_NEXT, "pause");
    puts("hehe");
    return r();
}
» gcc -shared -fPIC -o dlpause.so dlpause.c -ldl
»
```

sleep or backdoor?

```
» readlink /proc/1897499/exe
/usr/bin/sleep
»
```

sleep or backdoor?

```
» readlink /proc/1897499/exe
/usr/bin/sleep
» memgrep 1897499 backdoor
Backdoor? I prefer the term 'surprise entrance'.
»
```

sleep or backdoor?

```
» readlink /proc/1897499/exe
/usr/bin/sleep
» memgrep 1897499 backdoor
Backdoor? I prefer the term 'surprise entrance'.
» cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
»
```

sleep or backdoor?

```
» readlink /proc/1897499/exe
/usr/bin/sleep
» memgrep 1897499 backdoor
Backdoor? I prefer the term 'surprise entrance'.
» cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
» cat /proc/1897499/environ | tr '\0' '\n' | grep LD_PRELOAD
»
```

sleep or backdoor?

```
» readlink /proc/1897499/exe
/usr/bin/sleep
» memgrep 1897499 backdoor
Backdoor? I prefer the term 'surprise entrance'.
» cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
» cat /proc/1897499/environ | tr '\0' '\n' | grep LD_PRELOAD
» cat /proc/1897499/environ | tr '\0' '\n' | grep LD_LIBRARY_PATH
LD_LIBRARY_PATH=/home/aivarsk/hehe:
»
```

sleep or backdoor?

```
» cat /proc/1897499/maps | grep hehe
738209e00000-738209e28000 r--p 00000000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
738209e28000-738209fbd000 r-xp 00028000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
738209fbd000-73820a00c000 r--p 001bd000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a00c000-73820a010000 r--p 0020b000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a010000-73820a012000 rw-p 0020f000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a01f000-73820a020000 r--p 00214000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
»
```

sleep or backdoor?

```
» cat /proc/1897499/maps | grep hehe
738209e00000-738209e28000 r--p 00000000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
738209e28000-738209fbd000 r-xp 00028000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
738209fbd000-73820a00c000 r--p 001bd000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a00c000-73820a010000 r--p 0020b000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a010000-73820a012000 rw-p 0020f000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
73820a01f000-73820a020000 r--p 00214000 103:06 6720025
↪ /home/aivarsk/hehe/libc.so.6
» md5sum /lib/x86_64-linux-gnu/libc.so.6  /home/aivarsk/hehe/libc.so.6
1a6c7860478353176a19adb5a5bd7eac  /lib/x86_64-linux-gnu/libc.so.6
f8e7f9fbe2d9b4e726ab12c89d776ba4  /home/aivarsk/hehe/libc.so.6
»
```

Can we trust the environ?

```
» readlink /proc/1904234/exe
/usr/bin/sleep
»
```

Can we trust the environ?

```
» readlink /proc/1904234/exe
/usr/bin/sleep
» memgrep 1904234 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
»
```

Can we trust the environ?

```
» readlink /proc/1904234/exe
/usr/bin/sleep
» memgrep 1904234 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /proc/1904234/environ | tr '\0' '\n'
NOTHING_TO_SEE_HERE=move_along
TOTALLY_LEGIT=yes
»
```

Can we trust the environ?

```
» readlink /proc/1904234/exe
/usr/bin/sleep
» memgrep 1904234 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /proc/1904234/environ | tr '\0' '\n'
NOTHING_TO_SEE_HERE=move_along
TOTALLY_LEGIT=yes
» cat /proc/1904234/maps | grep hehe
75cd37266000-75cd37267000 r--p 00000000 103:06 6720023
↪ /home/aivarsk/hehe/dlpauseenviron.so
75cd37267000-75cd37268000 r-xp 00001000 103:06 6720023
↪ /home/aivarsk/hehe/dlpauseenviron.so
75cd37268000-75cd37269000 r--p 00002000 103:06 6720023
↪ /home/aivarsk/hehe/dlpauseenviron.so
75cd37269000-75cd3726a000 r--p 00002000 103:06 6720023
↪ /home/aivarsk/hehe/dlpauseenviron.so
75cd3726a000-75cd3726b000 rw-p 00003000 103:06 6720023
↪ /home/aivarsk/hehe/dlpauseenviron.so
»
```

Can we trust the environ?

```
» cat dlpauseenviron.c
#define _GNU_SOURCE
#include <dlfcn.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/prctl.h>
const char msg[] = "Backdoor? I prefer the term 'surprise entrance'.";
int pause(void) {
     char *e = malloc(128);
     memcpy(e, "NOTHING_TO_SEE_HERE=move_along\0TOTALLY_LEGIT=yes\0", 49);
     prctl(PR_SET_MM, PR_SET_MM_ENV_START, e, 0, 0);
     prctl(PR_SET_MM, PR_SET_MM_ENV_END, e + 49, 0, 0);
     static int (*r)(void);
     if (!r) r = dlsym(RTLD_NEXT, "pause");
     puts("hehe");
     return r();
}
» gcc -shared -fPIC -o dlpauseenviron.so dlpauseenviron.c -ldl
»
```

Can we trust the environ?

```
» memgrep 1904234 LD_PRELOAD
LD_PRELOAD
LD_PRELOAD
LD_PRELOAD=./dlpauseenviron.so
»
```

Can we trust the environ? - KISS

```
» readlink /proc/1908359/exe
/usr/bin/sleep
»
```

Can we trust the environ? - KISS

```
» readlink /proc/1908359/exe
/usr/bin/sleep
» memgrep 1908359 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
»
```

Can we trust the environ? - KISS

```
» readlink /proc/1908359/exe
/usr/bin/sleep
» memgrep 1908359 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /proc/1908359/environ | tr '\0' '\n' | grep LD_
»
```

Can we trust the environ? - KISS

```
» readlink /proc/1908359/exe
/usr/bin/sleep
» memgrep 1908359 backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
» cat /proc/1908359/environ | tr '\0' '\n' | grep LD_
» cat /proc/1908359/maps | grep hehe
72bc0a0d6000-72bc0a0d7000 r--p 00000000 103:06 6720026
↪ /home/aivarsk/hehe/dlpausehide.so
72bc0a0d7000-72bc0a0d8000 r-xp 00001000 103:06 6720026
↪ /home/aivarsk/hehe/dlpausehide.so
72bc0a0d8000-72bc0a0d9000 r--p 00002000 103:06 6720026
↪ /home/aivarsk/hehe/dlpausehide.so
72bc0a0d9000-72bc0a0da000 r--p 00002000 103:06 6720026
↪ /home/aivarsk/hehe/dlpausehide.so
72bc0a0da000-72bc0a0db000 rw-p 00003000 103:06 6720026
↪ /home/aivarsk/hehe/dlpausehide.so
```

Can we trust the environ? - KISS

```
» memgrep 1908359 LD_PRELOAD
LD_PRELOAD=
LD_PRELOAD=
LD_PRELOAD
LD_PRELOAD
»
```

Can we trust the environ? - KISS

```
» memgrep 1908359 LD_PRELOAD
LD_PRELOAD=
LD_PRELOAD=
LD_PRELOAD
LD_PRELOAD
» memgrep 1908359 LD_LIBRARY_PATH
LD_LIBRARY_PATH
LD_LIBRARY_PATH
                      variable LD_LIBRARY_PATH
»
»
```

Can we trust the environ? - KISS

```
» memgrep 1908359 LD_PRELOAD
LD_PRELOAD=
LD_PRELOAD=
LD_PRELOAD
LD_PRELOAD
» memgrep 1908359 LD_LIBRARY_PATH
LD_LIBRARY_PATH
LD_LIBRARY_PATH
                      variable LD_LIBRARY_PATH
»
» cat /proc/1908359/environ | tr '\0' '\n'  | grep MOVE
MOVEALONG=1
»
```

Can we trust the environ? - KISS

```
» cat dlpausehide.c
#define _GNU_SOURCE
#include <dlfcn.h>
#include <stdio.h>
#include <string.h>
extern char **environ;
const char msg[] = "Backdoor? I prefer the term 'surprise entrance'.";
int pause(void) {
     for (int i =0; environ[i]; i++) {
          if (strncmp(environ[i], "LD_PRELOAD=", 11) == 0) {
               memset(environ[i], ' ', strlen(environ[i]));
               strcpy(environ[i], "MOVEALONG=1");
          }
     }
     static int (*r)(void);
     if (!r) r = dlsym(RTLD_NEXT, "pause");
     puts("hehe");
     return r();
}
» gcc -shared -fPIC -o dlpausehide.so dlpausehide.c -ldl
»
```

Enough with "what" is running.

What about "who" is running it?

Who?

```
» ps up 1397710
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
johndoe  1397710  0.0  0.0   8360  2216 pts/45   S    08:55   0:00 /var/tmp/pwn inf
»
```

Who?

```
» ps up 1397710
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
johndoe  1397710  0.0  0.0   8360  2216 pts/45   S    08:55   0:00 /var/tmp/pwn inf
» ls -l /var/tmp/pwn
-rwsr-sr-x 1 johndoe johndoe 35416 Oct  8 08:44 /var/tmp/pwn
»
```

Who?

```
» ps up 1397710
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
johndoe  1397710  0.0  0.0   8360  2216 pts/45   S    08:55   0:00 /var/tmp/pwn inf
» ls -l /var/tmp/pwn
-rwsr-sr-x 1 johndoe johndoe 35416 Oct  8 08:44 /var/tmp/pwn
» ps up 2534158
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root     2534158  0.0  0.0  12884  4476 pts/62   S+   01:55   0:00 passwd
```

Real, effective, saved set, and filesystem UIDs (GIDs).

```
» cat /proc/1397710/status | grep -E 'Uid|Gid'
Uid:    1000    1002    1002    1002
Gid:    1000    1002    1002    1002
»
```

Real, effective, saved set, and filesystem UIDs (GIDs).

```
» cat /proc/1397710/status | grep -E 'Uid|Gid'
Uid:    1000    1002    1002    1002
Gid:    1000    1002    1002    1002
» id -nu 1000
aivarsk
»
```

Real, effective, saved set, and filesystem UIDs (GIDs).

```
» cat /proc/1397710/status | grep -E 'Uid|Gid'
Uid:    1000    1002    1002    1002
Gid:    1000    1002    1002    1002
» id -nu 1000
aivarsk
» id -nu 1002
johndoe
»
```

Does it matter who?

```
» cat shadow.c
#include <stdio.h>
#include <unistd.h>
int main() {
     FILE *f = fopen("/etc/shadow", "r");
     if (f == NULL) {
          perror("failed to open shadow");
     } else {
          char c;
          while ((c = fgetc(f)) != EOF)
               putchar(c);
          fclose(f);
          sleep(2147447412);
     }
}
»
```

Does it matter who?

```
» cat shadow.c
#include <stdio.h>
#include <unistd.h>
int main() {
     FILE *f = fopen("/etc/shadow", "r");
     if (f == NULL) {
          perror("failed to open shadow");
     } else {
          char c;
          while ((c = fgetc(f)) != EOF)
               putchar(c);
          fclose(f);
          sleep(2147447412);
     }
}
» gcc -Wall -o shadow shadow.c
»
```

Does it matter who?

```
» cat shadow.c
#include <stdio.h>
#include <unistd.h>
int main() {
     FILE *f = fopen("/etc/shadow", "r");
     if (f == NULL) {
          perror("failed to open shadow");
     } else {
          char c;
          while ((c = fgetc(f)) != EOF)
               putchar(c);
          fclose(f);
          sleep(2147447412);
     }
}
» gcc -Wall -o shadow shadow.c
» # hidden magic
»
```

Does it matter who?

```
» /var/tmp/shadow
root:*:19837:0:99999:7:::
daemon:*:19837:0:99999:7:::
bin:*:19837:0:99999:7:::
sys:*:19837:0:99999:7:::
sync:*:19837:0:99999:7:::
games:*:19837:0:99999:7:::
man:*:19837:0:99999:7:::
...
»
```

Does it matter who?

```
» ps up 1921347
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1921347  0.0  0.0   2748  1636 pts/50   S    00:35   0:00 /var/tmp/shadow
»
```

Does it matter who?

```
» ps up 1921347
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1921347  0.0  0.0   2748  1636 pts/50   S    00:35   0:00 /var/tmp/shadow
» cat /proc/1921347/status | grep -E 'Uid|Gid'
Uid:    1000    1000    1000    1000
Gid:    1000    1000    1000    1000
»
```

CapInh|CapPrm|CapEff - inheritable, permitted, and effective capabilities(7)

```
» cat /proc/1921347/status | grep -E 'Cap'
CapInh: 0000000800000000
CapPrm: 0000000000200004
CapEff: 0000000000200004
CapBnd: 000001ffffffffff
CapAmb: 0000000000000000
»
```

magic revealed

```
» getcap /var/tmp/shadow
/var/tmp/shadow cap_dac_read_search,cap_sys_admin=ep
»
```

magic revealed

```
» getcap /var/tmp/shadow
/var/tmp/shadow cap_dac_read_search,cap_sys_admin=ep
» sudo setcap cap_sys_admin,cap_dac_read_search+ep /var/tmp/shadow
»
```

The final ~~boss~~ sleep

sleep or backdoor?

```
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420  1380 pts/0    S+   00:50   0:00 /usr/bin/sleep inf
»
```

sleep or backdoor?

```
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420  1380 pts/0    S+   00:50   0:00 /usr/bin/sleep inf
» readlink /proc/1924852/exe
/usr/bin/sleep
»
```

sleep or backdoor?

```
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420  1380 pts/0    S+   00:50   0:00 /usr/bin/sleep inf
» readlink /proc/1924852/exe
/usr/bin/sleep
» memgrep 1924852  backdoor
Backdoor? I prefer the term 'surprise entrance'.
Backdoor? I prefer the term 'surprise entrance'.
»
```

sleep or backdoor?

```
» cat /proc/1924852/maps
00400000-00401000 r--p 00000000 00:a5 954209                              /usr/bin/sleep
...
00404000-00405000 rw-p 00003000 00:a5 954209                              /usr/bin/sleep
7c264a844000-7c264a847000 rw-p 00000000 00:00 0
7c264a847000-7c264a86f000 r--p 00000000 00:a5 554768
↪ /usr/lib/x86_64-linux-gnu/libc.so.6
...
7c264aa2e000-7c264aa3b000 rw-p 00000000 00:00 0
7c264aa43000-7c264aa45000 rw-p 00000000 00:00 0
7c264aa45000-7c264aa47000 r--p 00000000 00:00 0                           [vvar]
7c264aa47000-7c264aa49000 r--p 00000000 00:00 0                           [vvar_vclock]
7c264aa49000-7c264aa4b000 r-xp 00000000 00:00 0                           [vdso]
7c264aa4b000-7c264aa4c000 r--p 00000000 00:a5 554748
↪ /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
...
7c264aa82000-7c264aa83000 rw-p 00000000 00:00 0
7ffff88c0000-7ffff88e1000 rw-p 00000000 00:00 0                           [stack]
ffffffffff600000-ffffffffff601000 --xp 00000000 00:00 0                   [vsyscall]
»
```

sleep or backdoor?

```
» readlink /proc/1924852/exe
/usr/bin/sleep
»
```

sleep or backdoor?

```
» readlink /proc/1924852/exe
/usr/bin/sleep
» cat /usr/bin/sleep | strings | grep -ai backdoor
»
```

sleep or backdoor?

```
» readlink /proc/1924852/exe
/usr/bin/sleep
» cat /usr/bin/sleep | strings | grep -ai backdoor
» cat /proc/1924852/exe | strings | grep -ai backdoor
Backdoor? I prefer the term 'surprise entrance'.
»
```

sleep or backdoor?

```
» readlink /proc/1924852/exe
/usr/bin/sleep
» cat /usr/bin/sleep | strings | grep -ai backdoor
» cat /proc/1924852/exe | strings | grep -ai backdoor
Backdoor? I prefer the term 'surprise entrance'.
» md5sum /proc/1924852/exe `readlink /proc/1924852/exe`
962ba807b2814df8a339cb00045a8a8e  /proc/1924852/exe
2b8ca12a8081d85a6dd75235cde8b8db  /usr/bin/sleep
»
```

A clue

```
» cat /proc/1924852/environ | tr '\0' '\n'
MAIL=/var/mail/fubar
USER=fubar
HOME=/home/fubar
LOGNAME=fubar
TERM=xterm
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
SHELL=/bin/sh
PWD=/
»
```

A clue

```
» cat /proc/1924852/environ | tr '\0' '\n'
MAIL=/var/mail/fubar
USER=fubar
HOME=/home/fubar
LOGNAME=fubar
TERM=xterm
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
SHELL=/bin/sh
PWD=/
» cat /proc/1924852/cgroup
0::/system.slice/docker-4d510e9f54cdeea53ed1fa7846df43ccf784cde47176eec906fe6406e3558d55.s
↪ cope
»
```

NSpid - descendant namespace process ID hierarchy

```
» cat /proc/1924852/status | grep -E 'NSpid'
NSpid:  1924852 26
»
```

NSpid - descendant namespace process ID hierarchy

```
» cat /proc/1924852/status | grep -E 'NSpid'
NSpid:  1924852 26
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420   100 pts/0    S    Oct10   0:00 /usr/bin/sleep inf
»
```

NSpid - descendant namespace process ID hierarchy

```
» cat /proc/1924852/status | grep -E 'NSpid'
NSpid:  1924852 26
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420   100 pts/0    S    Oct10   0:00 /usr/bin/sleep inf
» cat /proc/1924852/cgroup
0::/system.slice/docker-4d510e9f54cdeea53ed1fa7846df43ccf784cde47176eec906fe6406e3558d55.s
↪ cope
»
```

NSpid - descendant namespace process ID hierarchy

```
» cat /proc/1924852/status | grep -E 'NSpid'
NSpid:  1924852 26
» ps up 1924852
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
aivarsk  1924852  0.0  0.0   2420   100 pts/0    S    Oct10   0:00 /usr/bin/sleep inf
» cat /proc/1924852/cgroup
0::/system.slice/docker-4d510e9f54cdeea53ed1fa7846df43ccf784cde47176eec906fe6406e3558d55.s
↪ cope
» docker exec 4d510e9f54cd ps up 26
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
foobar        26  0.0  0.0   2420   100 pts/0    S    Oct09   0:00 /usr/bin/sleep inf
»
```

/proc/pid/mountinfo - mount information

```
» cat /proc/1924852/mountinfo
14405 14331 0:165 / / rw,relatime - overlay overlay
↪ rw,lowerdir=/var/lib/docker/overlay2/l/5QO5HLLG2P4KD6IZSZCKJVSRYD:/var/lib/docker/overla
↪ y2/l/56S6INZQKNAEYAYRDZ4BTRQ2FH:/var/lib/docker/overlay2/l/UF3M4G3QEBDL2QYNHYDCAB6CDZ:/v
↪ ar/lib/docker/overlay2/l/F3QB2IV6EQEDJCHSPLCRUFDNHW:/var/lib/docker/overlay2/l/D3JSKDE6R
↪ 7FUYYQGYK6B7HEUOP:/var/lib/docker/overlay2/l/7HVX6Z6GRZ2D2D2RWBVIUCKU5Z:/var/lib/docker/
↪ overlay2/l/ZFVHZWCC4TWL5EYKQVBMKJXZ24:/var/lib/docker/overlay2/l/VV3PVGCZ7BKM4L5IFB3DUIP
↪ T2D:/var/lib/docker/overlay2/l/5ILVF7KOIVMMFMDYJ7YX2ZCOCP,upperdir=/var/lib/docker/overl
↪ ay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8c/diff,workdir=/var/l
↪ ib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8c/work
↪ ,nouserxattr
14407 14405 0:174 / /proc rw,nosuid,nodev,noexec,relatime - proc proc rw
14408 14405 0:175 / /dev rw,nosuid - tmpfs tmpfs rw,size=65536k,mode=755,inode64
14409 14408 0:176 / /dev/pts rw,nosuid,noexec,relatime - devpts devpts
↪ rw,gid=5,mode=620,ptmxmode=666
14410 14405 0:177 / /sys ro,nosuid,nodev,noexec,relatime - sysfs sysfs ro
14411 14410 0:29
↪ /system.slice/docker-4d510e9f54cdeea53ed1fa7846df43ccf784cde47176eec906fe6406e3558d55.sc
↪ ope /sys/fs/cgroup ro,nosuid,nodev,noexec,relatime - cgroup2 cgroup
↪ rw,nsdelegate,memory_recursiveprot
»
```

0152

Fixing the "broken" readlink

```
» sudo ls -l
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
-rwxr-xr-x 1 root root 15720 Oct 10 00:48
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
»
```

Fixing the "broken" readlink

```
» sudo ls -l
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
-rwxr-xr-x 1 root root 15720 Oct 10 00:48
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
» sudo md5sum
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
962ba807b2814df8a339cb00045a8a8e
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
»
```

Fixing the "broken" readlink

```
» sudo ls -l
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
-rwxr-xr-x 1 root root 15720 Oct 10 00:48
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
» sudo md5sum
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
962ba807b2814df8a339cb00045a8a8e
↪ /var/lib/docker/overlay2/86930b29816d5ed604cb9d235b752938cfaab1dab134c4e059171af2658d2a8
↪ c/diff/usr/bin/sleep
» md5sum /proc/1924852/exe `readlink /proc/1924852/exe`
962ba807b2814df8a339cb00045a8a8e  /proc/1924852/exe
2b8ca12a8081d85a6dd75235cde8b8db  /usr/bin/sleep
»
```



Glass Onion: A Knives Out Mystery (2022), directed by Rian Johnson. Distributed by Netflix.

Thank you!



microSRE.io

Aivars Kalvāns | aivars.kalvans@gmail.com | https://aivarsk.com