Evasive Linux Malware

Craig H. Rowland
Founder/CEO
@CraigHRowland

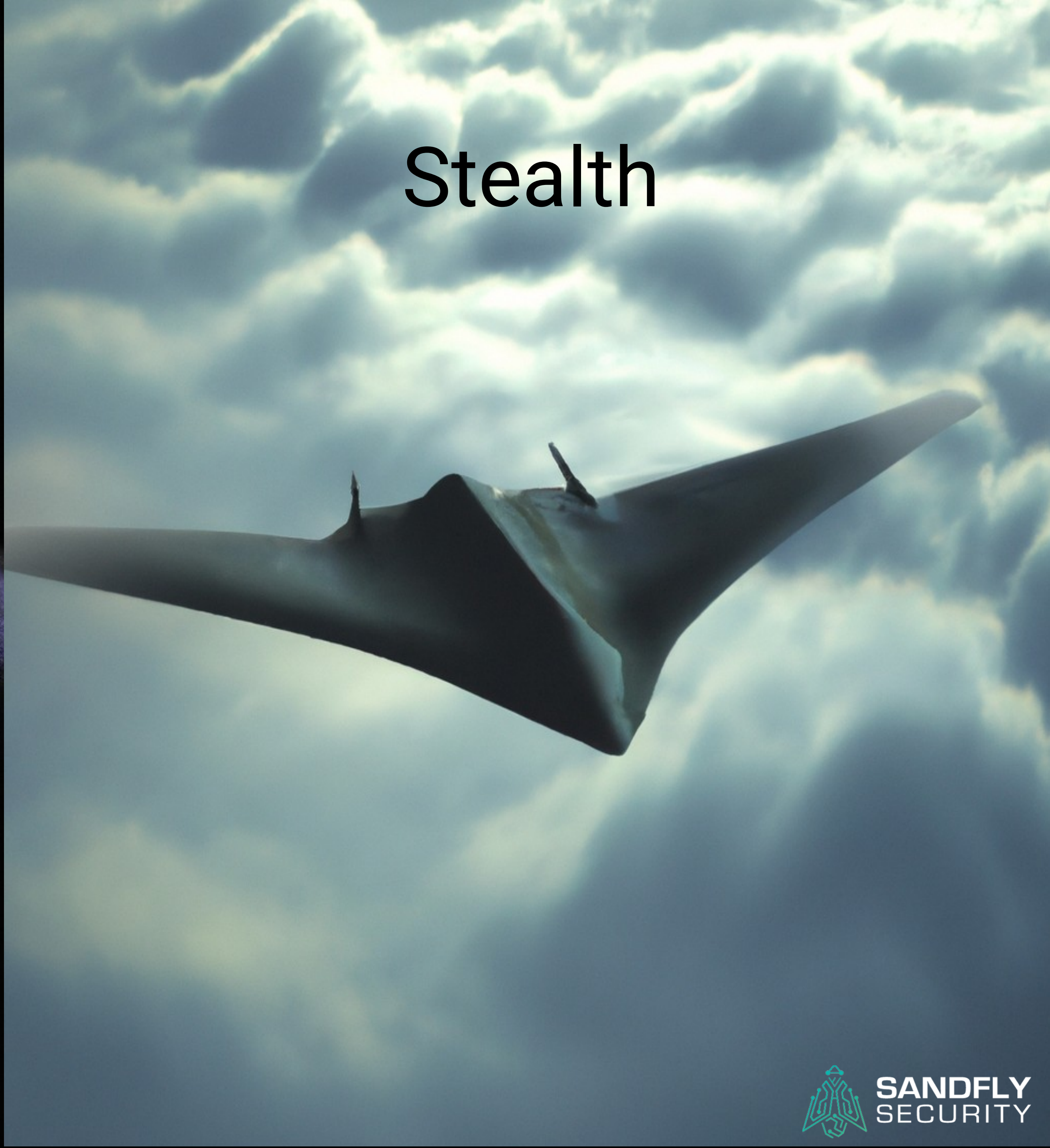
www.sandflysecurity.com
@SandflySecurity

When you visit Scandinavia:
When Scandinavia visits you:

Evasive malware uses simple tactics to avoid detection.

SANDFLY SECURITY

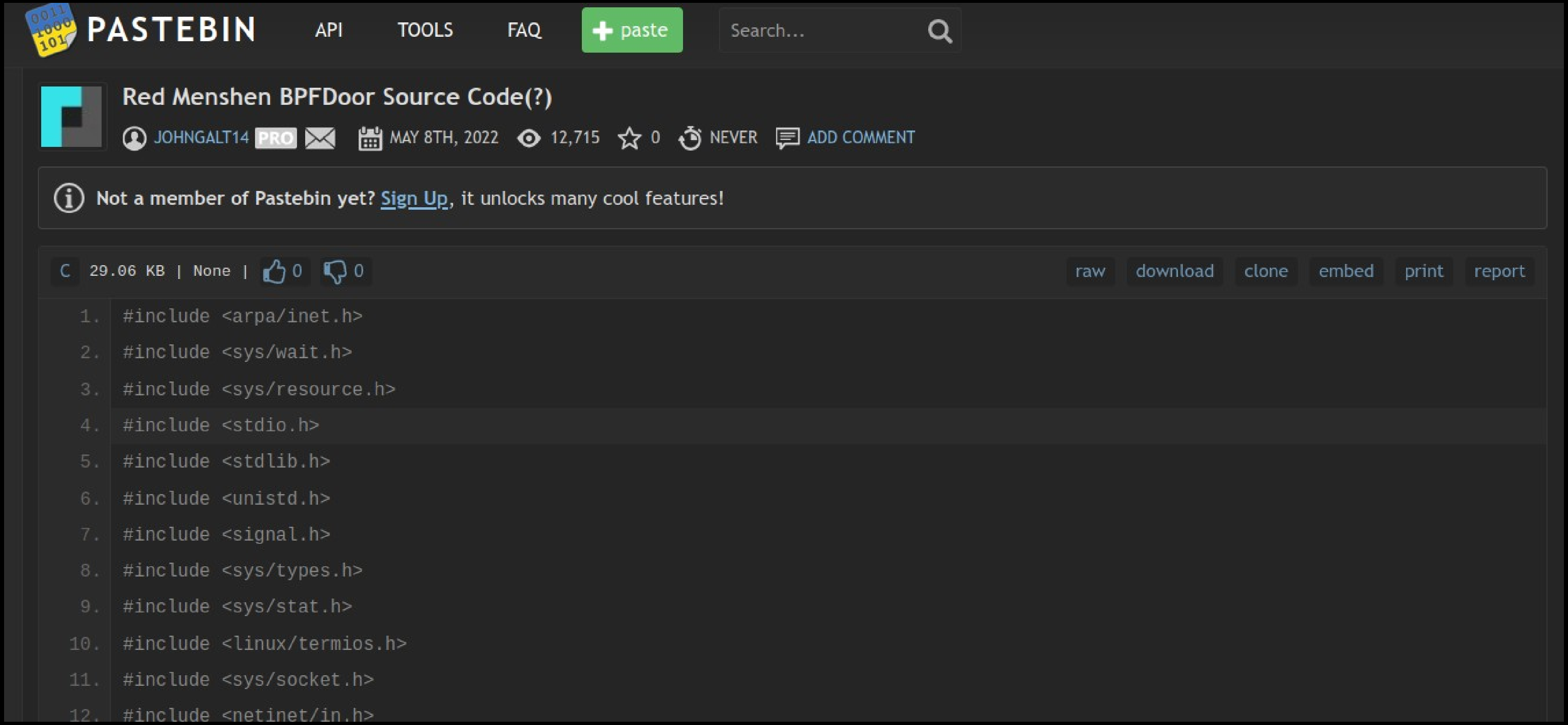
Evasive



Stealth

12:00

BPFDoor Dropped on Pastebin



Red Menshen BPFDoor Source Code(?)

JOHNGALT14 PRO MAY 8TH, 2022 12,715 0 NEVER ADD COMMENT

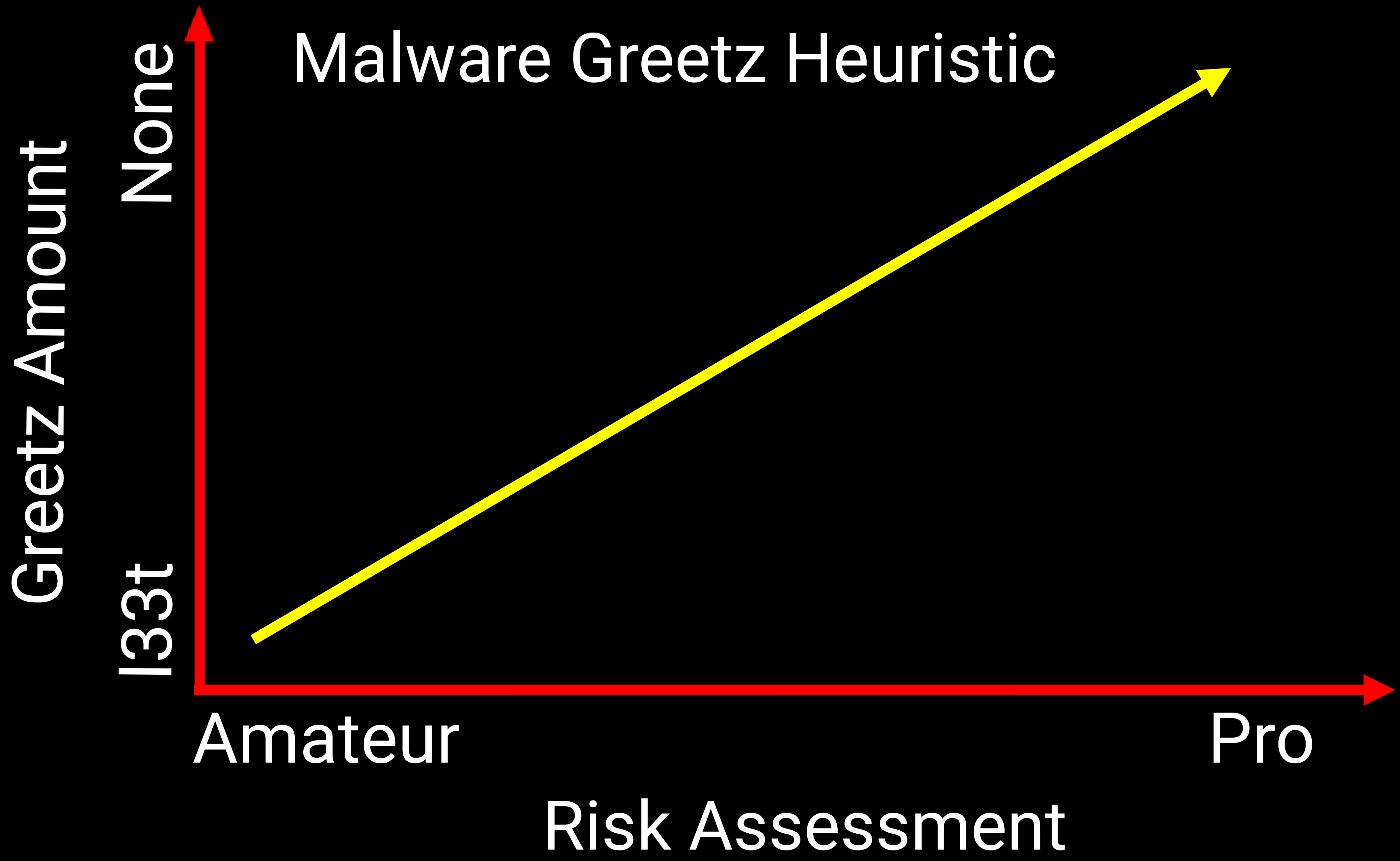
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

C 29.06 KB | None | 0 0

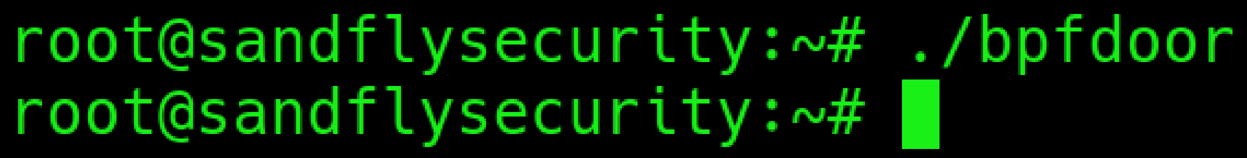
```c
#include <arpa/inet.h>
#include <sys/wait.h>
#include <sys/resource.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <signal.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <linux/termios.h>
#include <sys/socket.h>
#include <netinet/in.h>
```

https://pastebin.com/kmmJuuQP

Malware Greetz Heuristic



BPFDoor Executed



```
root@sandflysecurity:~# ./bpfdoor
root@sandflysecurity:~# 
```

BPFDoor Features

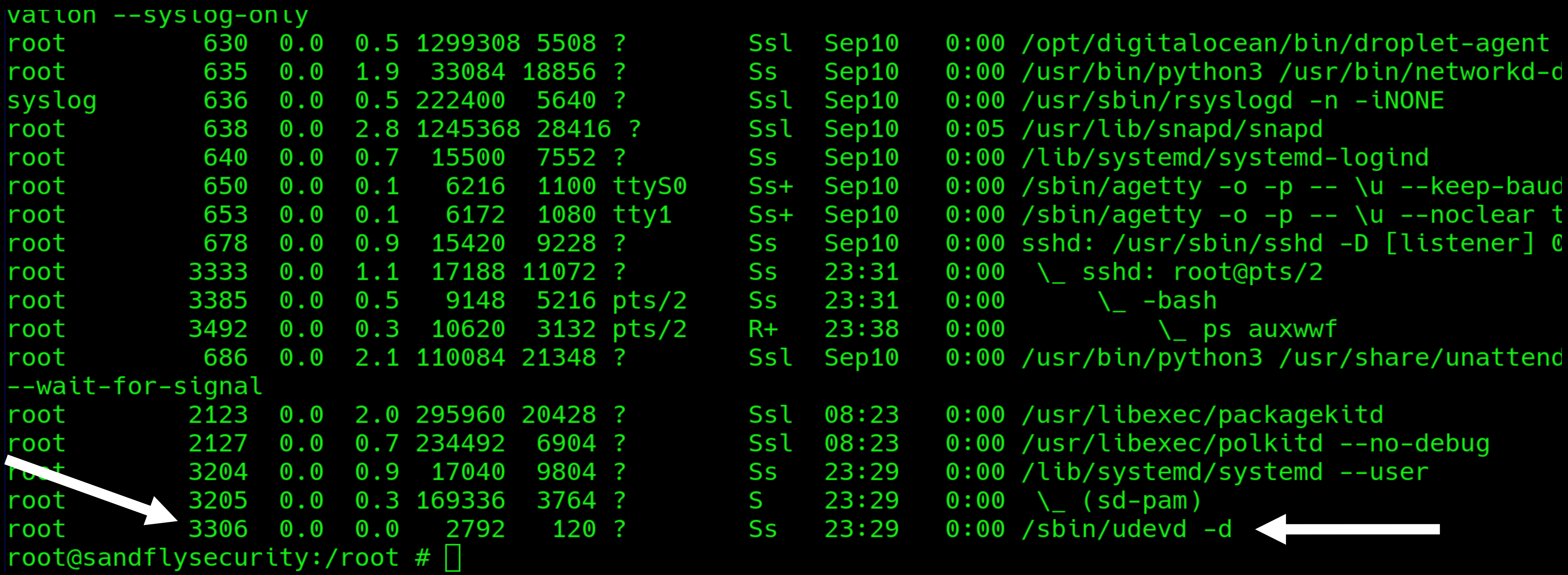
- Masquerading
- Bypasses Security
- Anti-Forensics
- Encrypted Comms
- Professional

Masquerading

Masquerading – BPFDoor Names Used

```
/sbin/udevd -d
/sbin/mingetty /dev/tty7
/usr/sbin/console-kit-daemon --no-daemon
hald-addon-acpi: listening on acpi kernel interface
/proc/acpi/event
dbus-daemon --system
hald-runner
pickup -l -t fifo -u
avahi-daemon: chroot helper
/sbin/auditd -n
/usr/lib/systemd/systemd-journald
```

Masquerading – Imposter Process

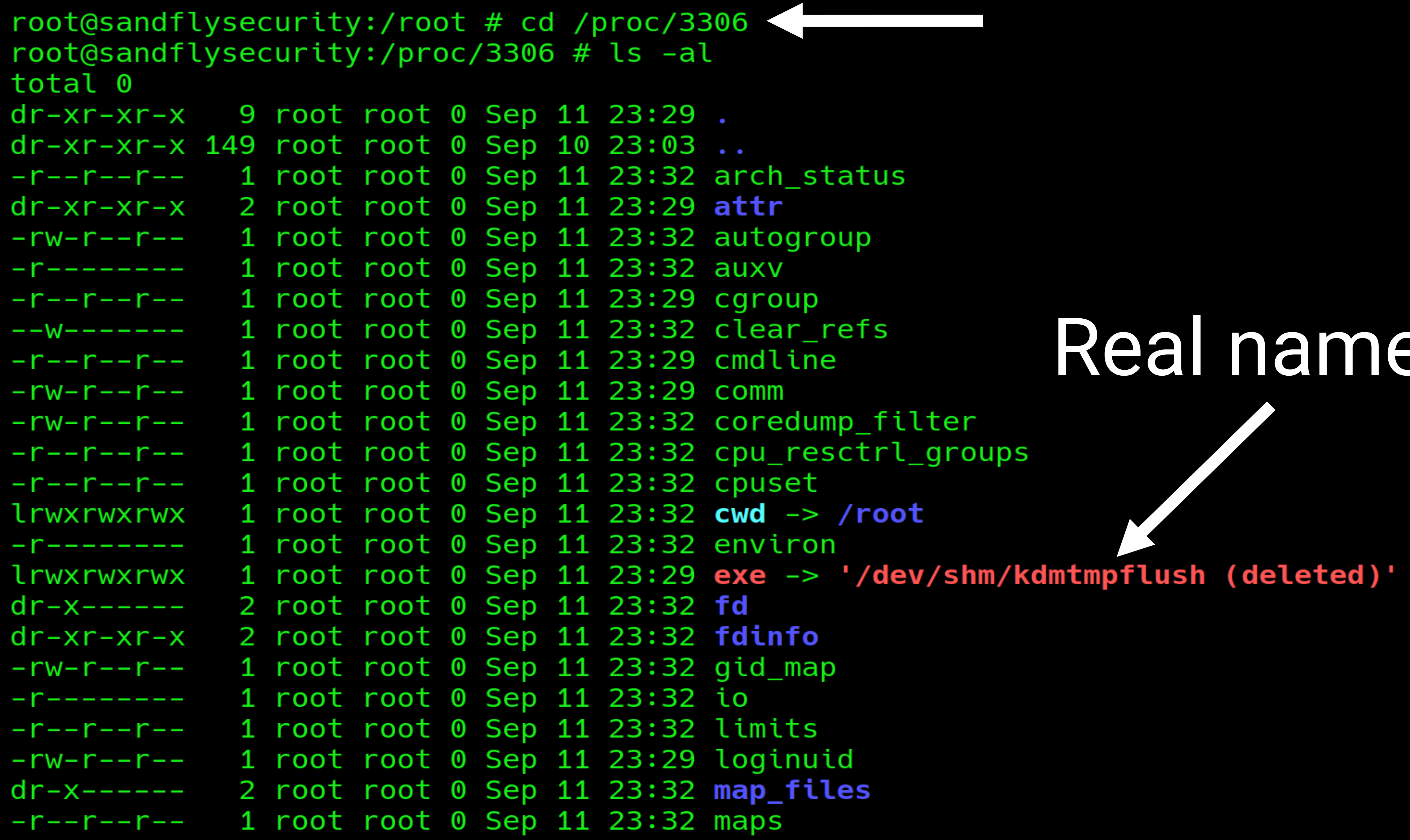


```
vation --syslog-only
root         630  0.0  0.5 1299308 5508 ?        Ssl  Sep10   0:00 /opt/digitalocean/bin/droplet-agent
root         635  0.0  1.9  33084 18856 ?        Ss   Sep10   0:00 /usr/bin/python3 /usr/bin/networkd-d
syslog       636  0.0  0.5 222400  5640 ?        Ssl  Sep10   0:00 /usr/sbin/rsyslogd -n -iNONE
root         638  0.0  2.8 1245368 28416 ?       Ssl  Sep10   0:05 /usr/lib/snapd/snapd
root         640  0.0  0.7  15500  7552 ?        Ss   Sep10   0:00 /lib/systemd/systemd-logind
root         650  0.0  0.1   6216  1100 ttyS0    Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --keep-baud
root         653  0.0  0.1   6172  1080 tty1     Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --noclear t
root         678  0.0  0.9  15420  9228 ?        Ss   Sep10   0:00 sshd: /usr/sbin/sshd -D [listener] 0
root        3333  0.0  1.1  17188 11072 ?        Ss   23:31   0:00  \_ sshd: root@pts/2
root        3385  0.0  0.5   9148  5216 pts/2    Ss   23:31   0:00      \_ -bash
root        3492  0.0  0.3  10620  3132 pts/2    R+   23:38   0:00          \_ ps auxwwf
root         686  0.0  2.1 110084 21348 ?        Ssl  Sep10   0:00 /usr/bin/python3 /usr/share/unattend
--wait-for-signal
root        2123  0.0  2.0 295960 20428 ?        Ssl  08:23   0:00 /usr/libexec/packagekitd
root        2127  0.0  0.7 234492  6904 ?        Ssl  08:23   0:00 /usr/libexec/polkitd --no-debug
root        3204  0.0  0.9  17040  9804 ?        Ss   23:29   0:00 /lib/systemd/systemd --user
root        3205  0.0  0.3 169336  3764 ?        S    23:29   0:00  \_ (sd-pam)
root        3306  0.0  0.0   2792   120 ?        Ss   23:29   0:00 /sbin/udevd -d
root@sandflysecurity:/root # 
```

Masquerading – Forensic Commands

```
ps -auxwwf

pstree

ls -al /proc/<PID>

strings  /proc/<PID>/comm

strings  /proc/<PID>/cmdline
```

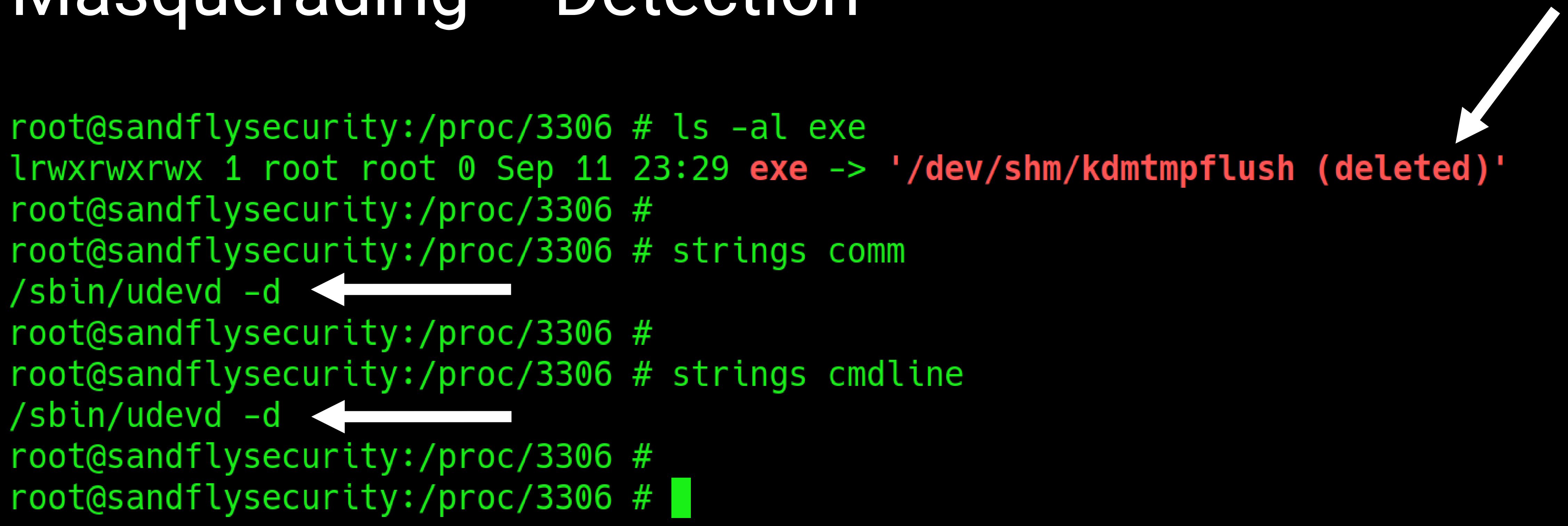
Masquerading – Detection



```
root@sandflysecurity:/root # cd /proc/3306
root@sandflysecurity:/proc/3306 # ls -al
total 0
dr-xr-xr-x   9 root root 0 Sep 11 23:29 .
dr-xr-xr-x 149 root root 0 Sep 10 23:03 ..
-r--r--r--   1 root root 0 Sep 11 23:32 arch_status
dr-xr-xr-x   2 root root 0 Sep 11 23:29 attr
-rw-r--r--   1 root root 0 Sep 11 23:32 autogroup
-r--------   1 root root 0 Sep 11 23:32 auxv
-r--r--r--   1 root root 0 Sep 11 23:29 cgroup
--w-------   1 root root 0 Sep 11 23:32 clear_refs
-r--r--r--   1 root root 0 Sep 11 23:29 cmdline
-rw-r--r--   1 root root 0 Sep 11 23:29 comm
-rw-r--r--   1 root root 0 Sep 11 23:32 coredump_filter
-r--r--r--   1 root root 0 Sep 11 23:32 cpu_resctrl_groups
-r--r--r--   1 root root 0 Sep 11 23:32 cpuset
lrwxrwxrwx   1 root root 0 Sep 11 23:32 cwd -> /root
-r--------   1 root root 0 Sep 11 23:32 environ
lrwxrwxrwx   1 root root 0 Sep 11 23:29 exe -> '/dev/shm/kdmtmpflush (deleted)'
dr-x------   2 root root 0 Sep 11 23:32 fd
dr-xr-xr-x   2 root root 0 Sep 11 23:32 fdinfo
-rw-r--r--   1 root root 0 Sep 11 23:32 gid_map
-r--------   1 root root 0 Sep 11 23:32 io
-r--r--r--   1 root root 0 Sep 11 23:32 limits
-rw-r--r--   1 root root 0 Sep 11 23:29 loginuid
dr-x------   2 root root 0 Sep 11 23:32 map_files
-r--r--r--   1 root root 0 Sep 11 23:32 maps
```

Real name.

Masquerading – Detection



```
root@sandflysecurity:/proc/3306 # ls -al exe
lrwxrwxrwx 1 root root 0 Sep 11 23:29 exe -> '/dev/shm/kdmtmpflush (deleted)'
root@sandflysecurity:/proc/3306 #
root@sandflysecurity:/proc/3306 # strings comm
/sbin/udevd -d
root@sandflysecurity:/proc/3306 #
root@sandflysecurity:/proc/3306 # strings cmdline
/sbin/udevd -d
root@sandflysecurity:/proc/3306 #
root@sandflysecurity:/proc/3306 #
```

Anti-Forensics

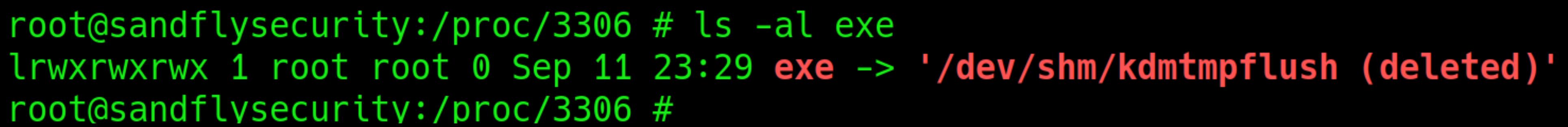
- Binary Deletion
- Environment Wipe
- Timestomping

Junior admins when they see a suspicious Linux process.

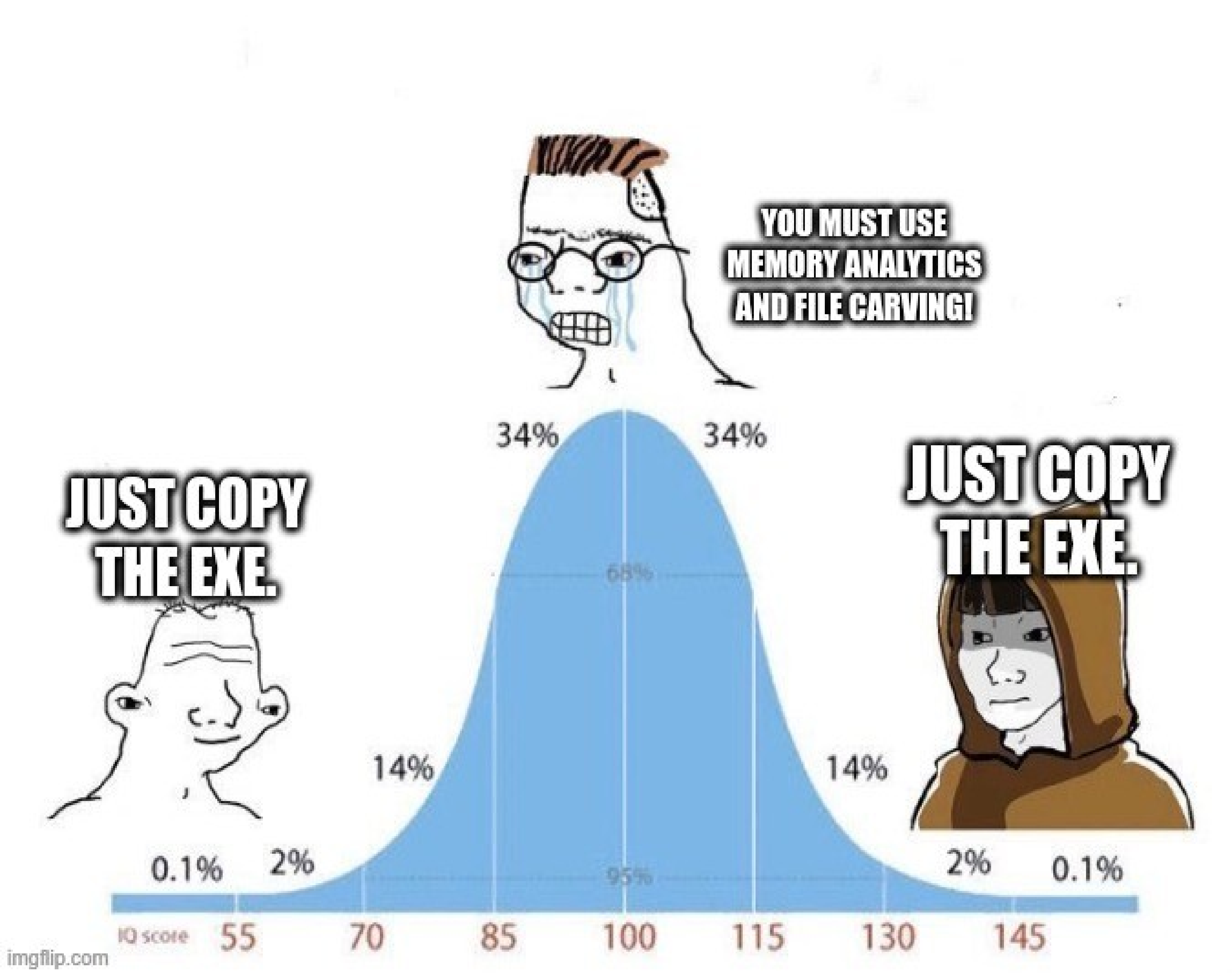
Never do this!

Binary Deletion

Anti-Forensics – Binary Deletion



```
root@sandflysecurity:/proc/3306 # ls -al exe
lrwxrwxrwx 1 root root 0 Sep 11 23:29 exe -> '/dev/shm/kdmtmpflush (deleted)'
root@sandflysecurity:/proc/3306 #
```



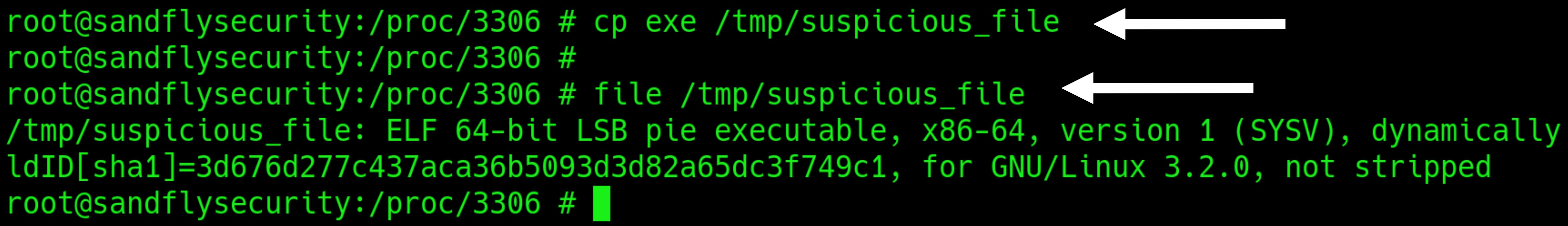
Binary Recovery

SANDFLY SECURITY

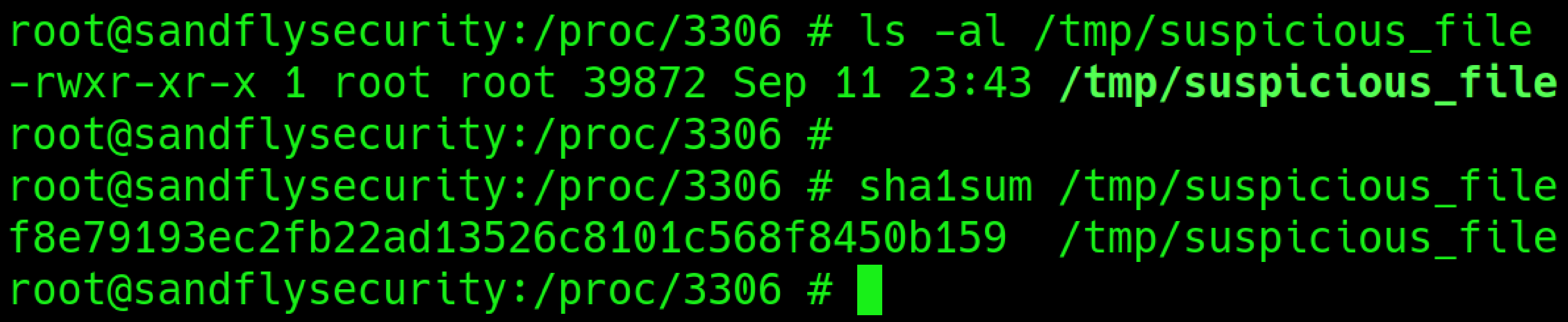
Anti-Forensics – Binary Recovery Commands

```
cp /proc/<PID>/exe /tmp/recovered_binary

sha1sum /tmp/recovered_binary

scp /proc/<PID>/exe user@ip_addr:~/recovered_binary
```

Anti-Forensics – Binary Recovery



```
root@sandflysecurity:/proc/3306 # cp exe /tmp/suspicious_file
root@sandflysecurity:/proc/3306 #
root@sandflysecurity:/proc/3306 # file /tmp/suspicious_file
/tmp/suspicious_file: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically
ldID[sha1]=3d676d277c437aca36b5093d3d82a65dc3f749c1, for GNU/Linux 3.2.0, not stripped
root@sandflysecurity:/proc/3306 #
```



```
root@sandflysecurity:/proc/3306 # ls -al /tmp/suspicious_file
-rwxr-xr-x 1 root root 39872 Sep 11 23:43 /tmp/suspicious_file
root@sandflysecurity:/proc/3306 #
root@sandflysecurity:/proc/3306 # sha1sum /tmp/suspicious_file
f8e79193ec2fb22ad13526c8101c568f8450b159  /tmp/suspicious_file
root@sandflysecurity:/proc/3306 #
```

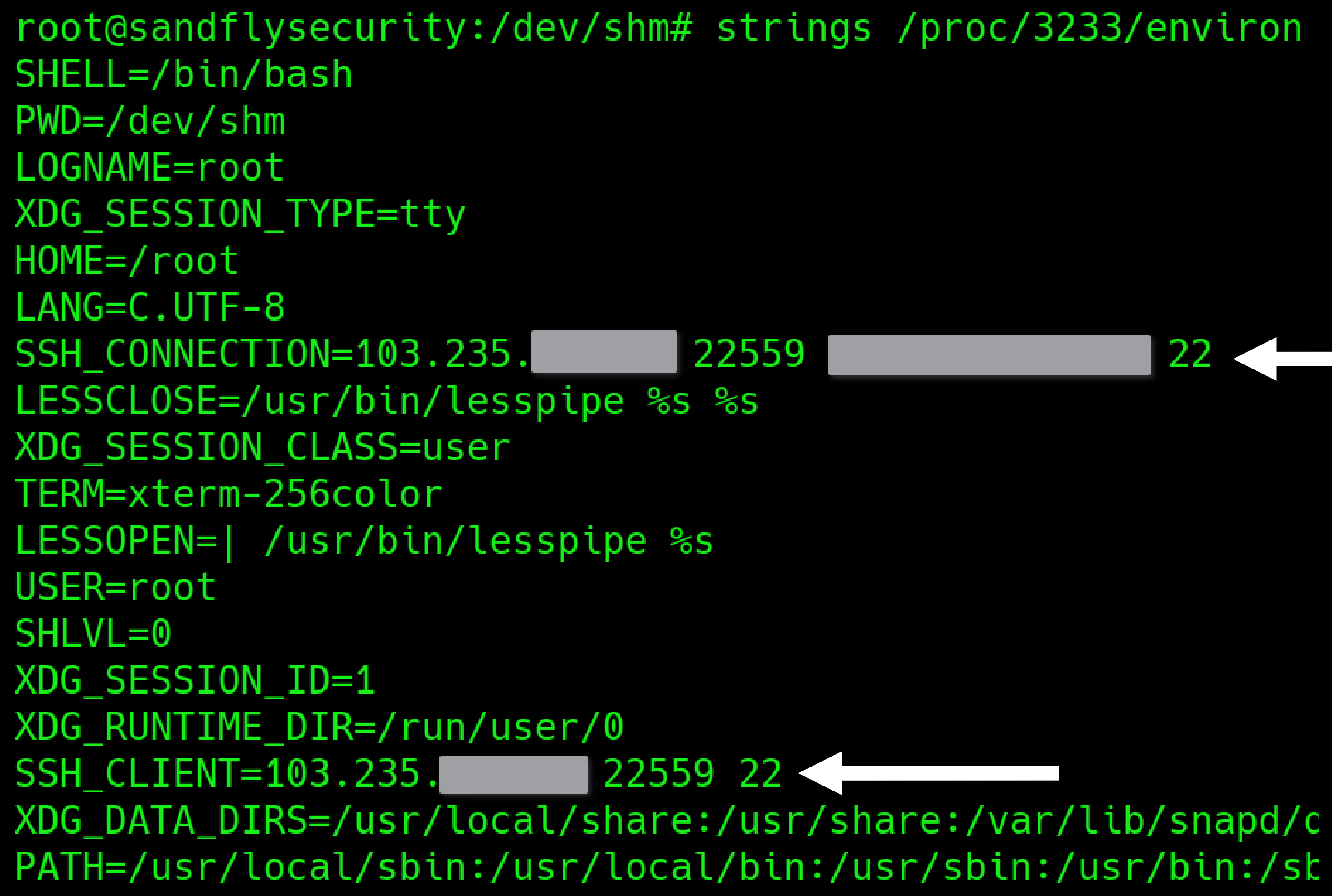
Environment Wipe

Anti-Forensics – Environment Commands

```
strings /proc/<PID>/environ

cat /proc/<PID>/environ | tr '\0' '\n'
```

SANDFLY SECURITY

Anti-Forensics – Normal Environment



```
root@sandflysecurity:/dev/shm# strings /proc/3233/environ
SHELL=/bin/bash
PWD=/dev/shm
LOGNAME=root
XDG_SESSION_TYPE=tty
HOME=/root
LANG=C.UTF-8
SSH_CONNECTION=103.235.[redacted] 22559 [redacted] 22
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=root
SHLVL=0
XDG_SESSION_ID=1
XDG_RUNTIME_DIR=/run/user/0
SSH_CLIENT=103.235.[redacted] 22559 22
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/c
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sb
```

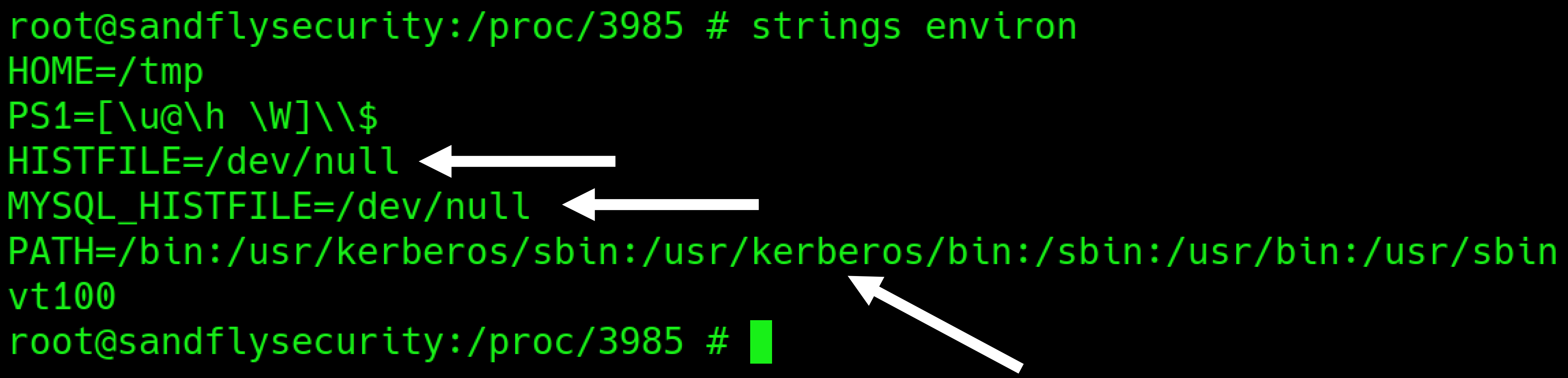
SANDFLY SECURITY

Anti-Forensics – BPFDoor Environment Wiped

```
root@sandflysecurity:/proc/3306 # strings environ
root@sandflysecurity:/proc/3306 # █
```

¯_(ツ)_/¯

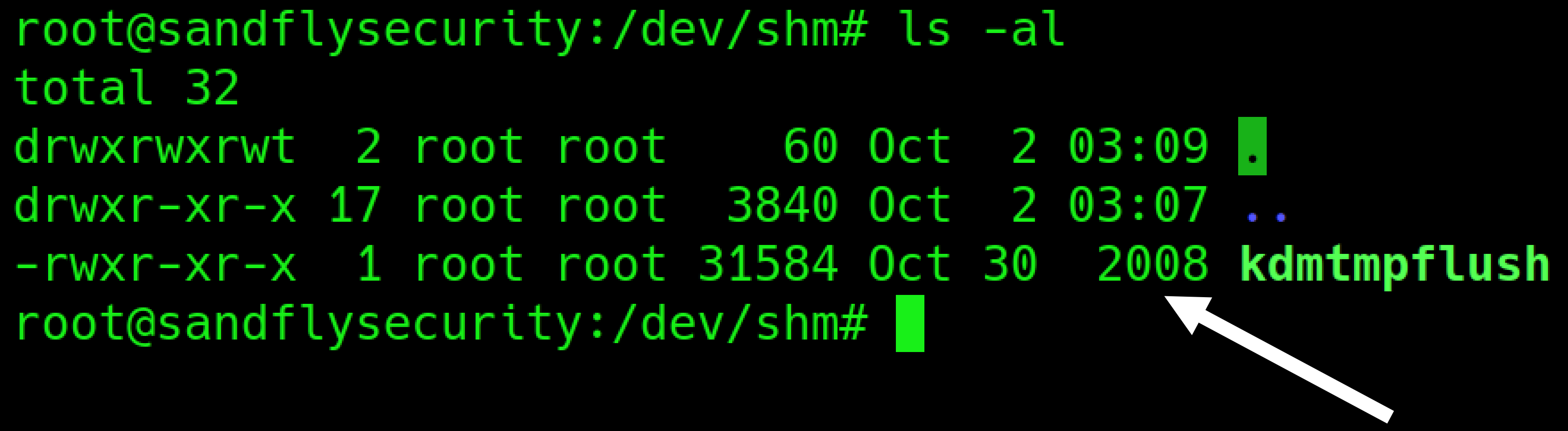
Anti-Forensics – BPFDoor Shell Environment



```
root@sandflysecurity:/proc/3985 # strings environ
HOME=/tmp
PS1=[\u@\h \W]\\$
HISTFILE=/dev/null
MYSQL_HISTFILE=/dev/null
PATH=/bin:/usr/kerberos/sbin:/usr/kerberos/bin:/sbin:/usr/bin:/usr/sbin
vt100
root@sandflysecurity:/proc/3985 #
```

Timestomping

Anti-Forensics – Timestomping



```
root@sandflysecurity:/dev/shm# ls -al
total 32
drwxrwxrwt  2 root root    60 Oct  2 03:09 .
drwxr-xr-x 17 root root  3840 Oct  2 03:07 ..
-rwxr-xr-x  1 root root 31584 Oct 30  2008 kdmtmpflush
root@sandflysecurity:/dev/shm# 
```

Bypasses Security

Photo credit: Wisconsin DNR

How to be Seen

- Clumsy security disabling.
- Make system unstable.
- Weird network traffic.

SANDFLY SECURITY

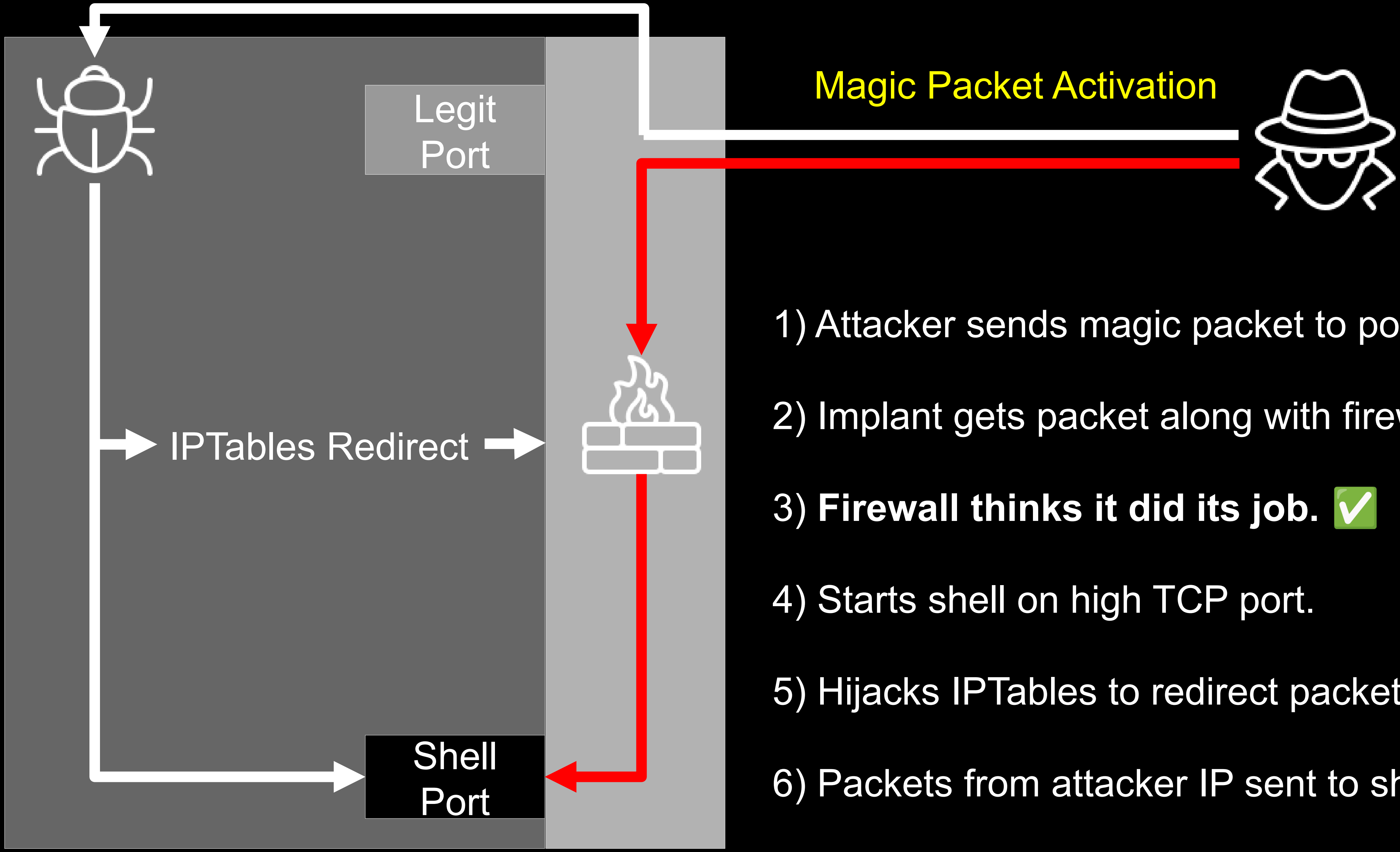
How to Hide

+ Disable only what's needed.

+ Focused and low impact.

+ Covert communications.

SANDFLY SECURITY



1) Attacker sends magic packet to port.

2) Implant gets packet along with firewall.

3) **Firewall thinks it did its job.** ✅

4) Starts shell on high TCP port.

5) Hijacks IPTables to redirect packets.

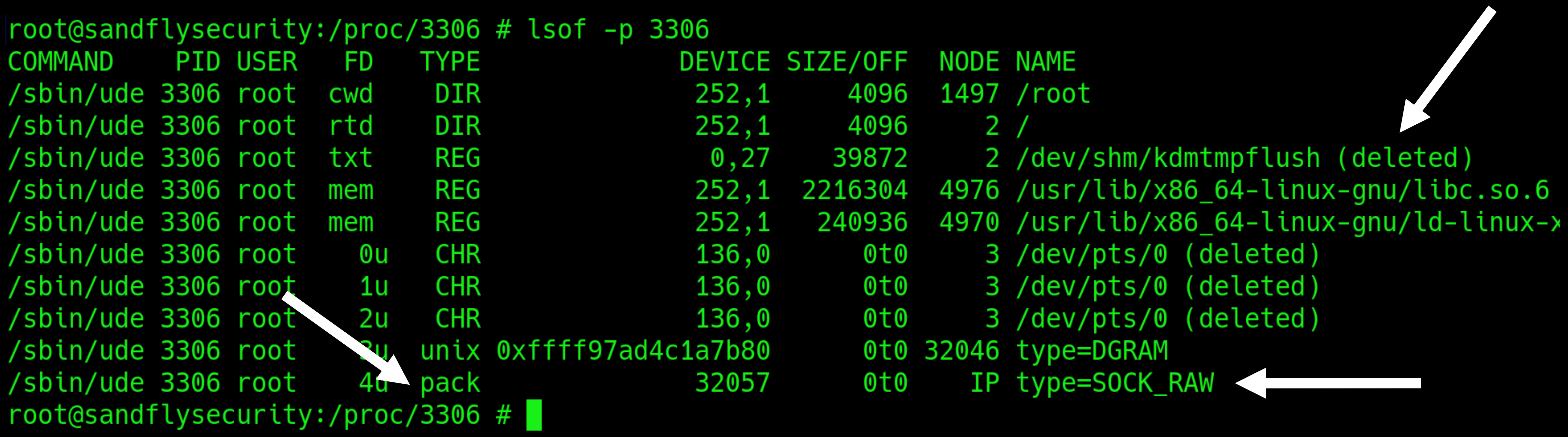
6) Packets from attacker IP sent to shell.

SANDFLY SECURITY

Bypasses Security – Sniffer Detection Commands

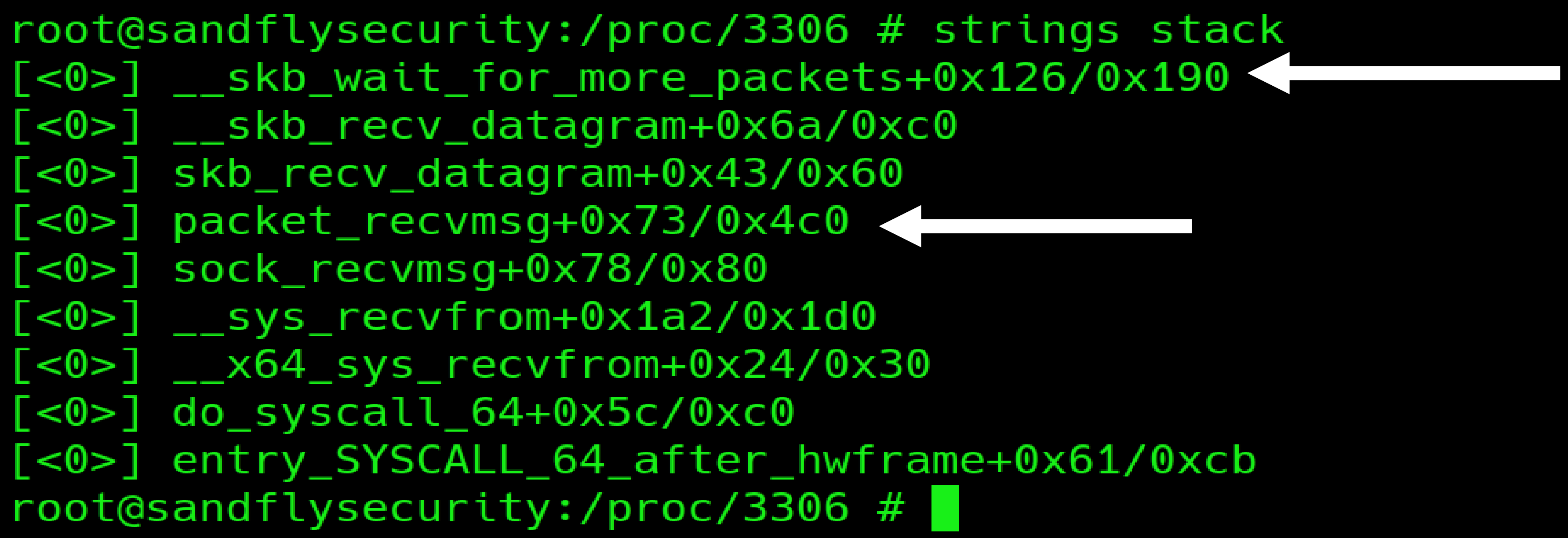
```
lsof -p <PID>

ss -0bp

cat /proc/<PID>/stack

ls /proc/<PID>/fd
```

Bypasses Security – Sniffer Sockets w/lsof



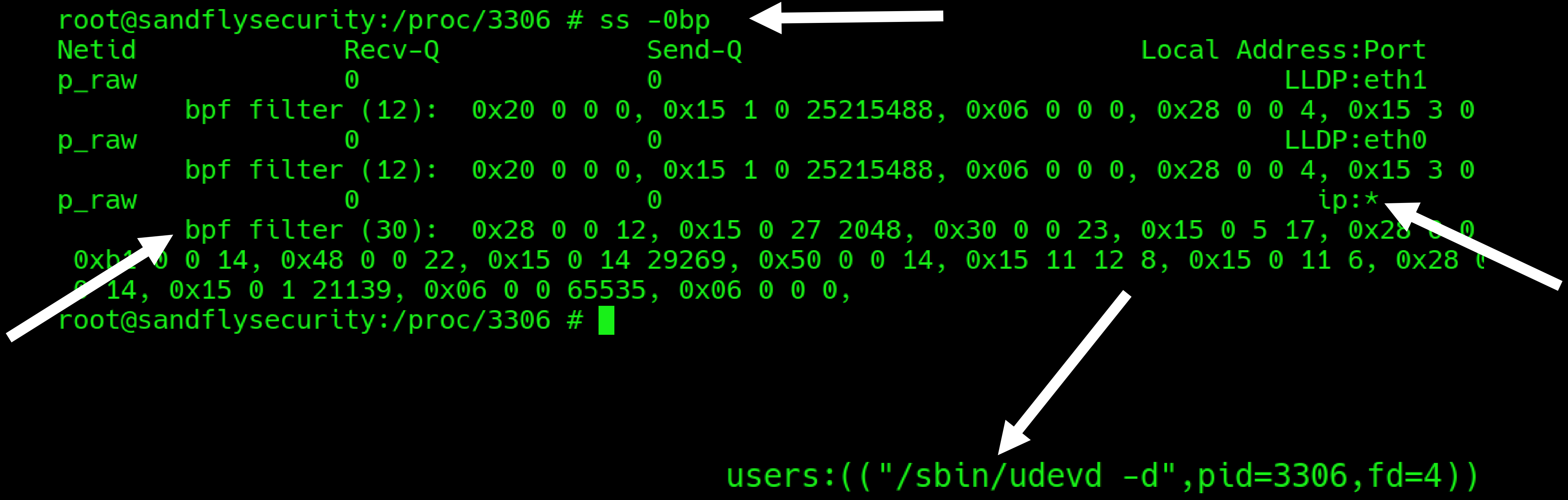
```
root@sandflysecurity:/proc/3306 # lsof -p 3306
COMMAND    PID USER   FD    TYPE             DEVICE SIZE/OFF  NODE NAME
/sbin/ude 3306 root  cwd     DIR              252,1     4096  1497 /root
/sbin/ude 3306 root  rtd     DIR              252,1     4096     2 /
/sbin/ude 3306 root  txt     REG               0,27    39872     2 /dev/shm/kdmtmpflush (deleted)
/sbin/ude 3306 root  mem     REG              252,1  2216304  4976 /usr/lib/x86_64-linux-gnu/libc.so.6
/sbin/ude 3306 root  mem     REG              252,1   240936  4970 /usr/lib/x86_64-linux-gnu/ld-linux-x
/sbin/ude 3306 root    0u    CHR              136,0      0t0     3 /dev/pts/0 (deleted)
/sbin/ude 3306 root    1u    CHR              136,0      0t0     3 /dev/pts/0 (deleted)
/sbin/ude 3306 root    2u    CHR              136,0      0t0     3 /dev/pts/0 (deleted)
/sbin/ude 3306 root    3u   unix 0xffff97ad4c1a7b80      0t0 32046 type=DGRAM
/sbin/ude 3306 root    4u   pack              32057      0t0    IP type=SOCK_RAW
root@sandflysecurity:/proc/3306 #
```

Bypasses Security – Sniffer Stack Trace



```
root@sandflysecurity:/proc/3306 # strings stack
[<0>] __skb_wait_for_more_packets+0x126/0x190
[<0>] __skb_recv_datagram+0x6a/0xc0
[<0>] skb_recv_datagram+0x43/0x60
[<0>] packet_recvmsg+0x73/0x4c0
[<0>] sock_recvmsg+0x78/0x80
[<0>] __sys_recvfrom+0x1a2/0x1d0
[<0>] __x64_sys_recvfrom+0x24/0x30
[<0>] do_syscall_64+0x5c/0xc0
[<0>] entry_SYSCALL_64_after_hwframe+0x61/0xcb
root@sandflysecurity:/proc/3306 #
```

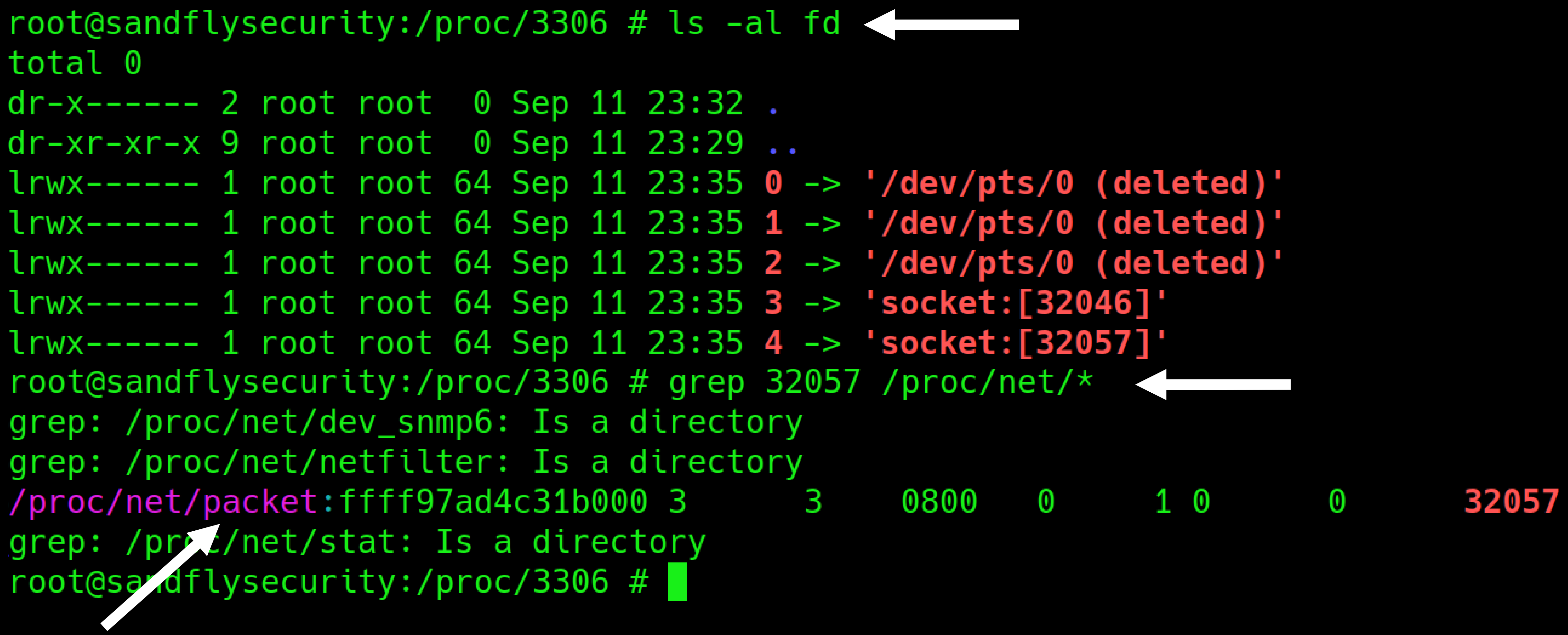
Bypasses Security – Sniffer BPF Filter



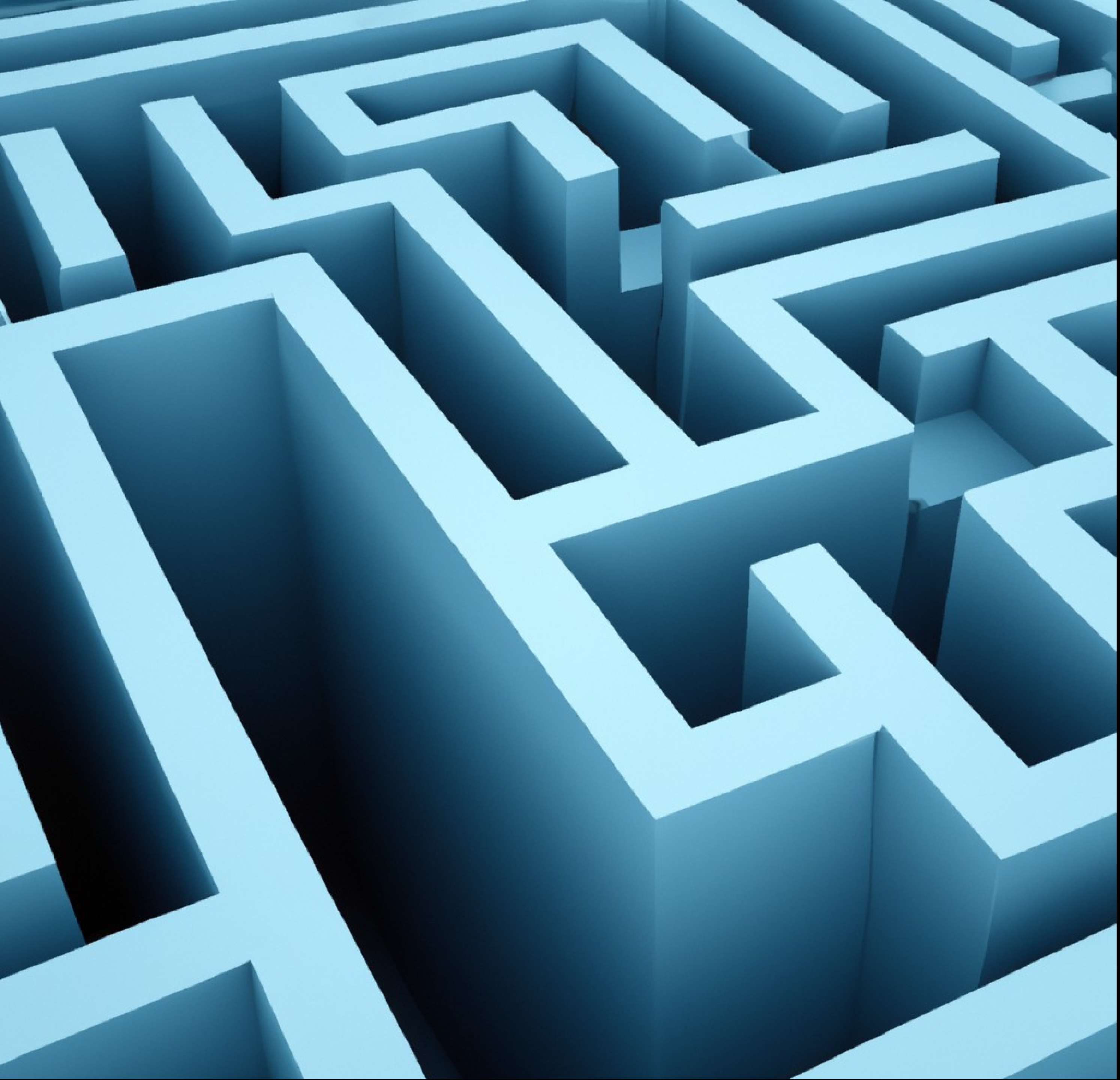
```
root@sandflysecurity:/proc/3306 # ss -0bp
Netid                 Recv-Q                 Send-Q                           Local Address:Port
p_raw                 0                      0                                         LLDP:eth1
        bpf filter (12):  0x20 0 0 0, 0x15 1 0 25215488, 0x06 0 0 0, 0x28 0 0 4, 0x15 3 0
p_raw                 0                      0                                         LLDP:eth0
        bpf filter (12):  0x20 0 0 0, 0x15 1 0 25215488, 0x06 0 0 0, 0x28 0 0 4, 0x15 3 0
p_raw                 0                      0                                           ip:*
        bpf filter (30):  0x28 0 0 12, 0x15 0 27 2048, 0x30 0 0 23, 0x15 0 5 17, 0x28 0 0
 0xb1 0 0 14, 0x48 0 0 22, 0x15 0 14 29269, 0x50 0 0 14, 0x15 11 12 8, 0x15 0 11 6, 0x28 0
 0 14, 0x15 0 1 21139, 0x06 0 0 65535, 0x06 0 0 0,
root@sandflysecurity:/proc/3306 #
```

```
users:(("/sbin/udevd -d",pid=3306,fd=4))
```

Bypasses Security – Sniffer File Descriptors

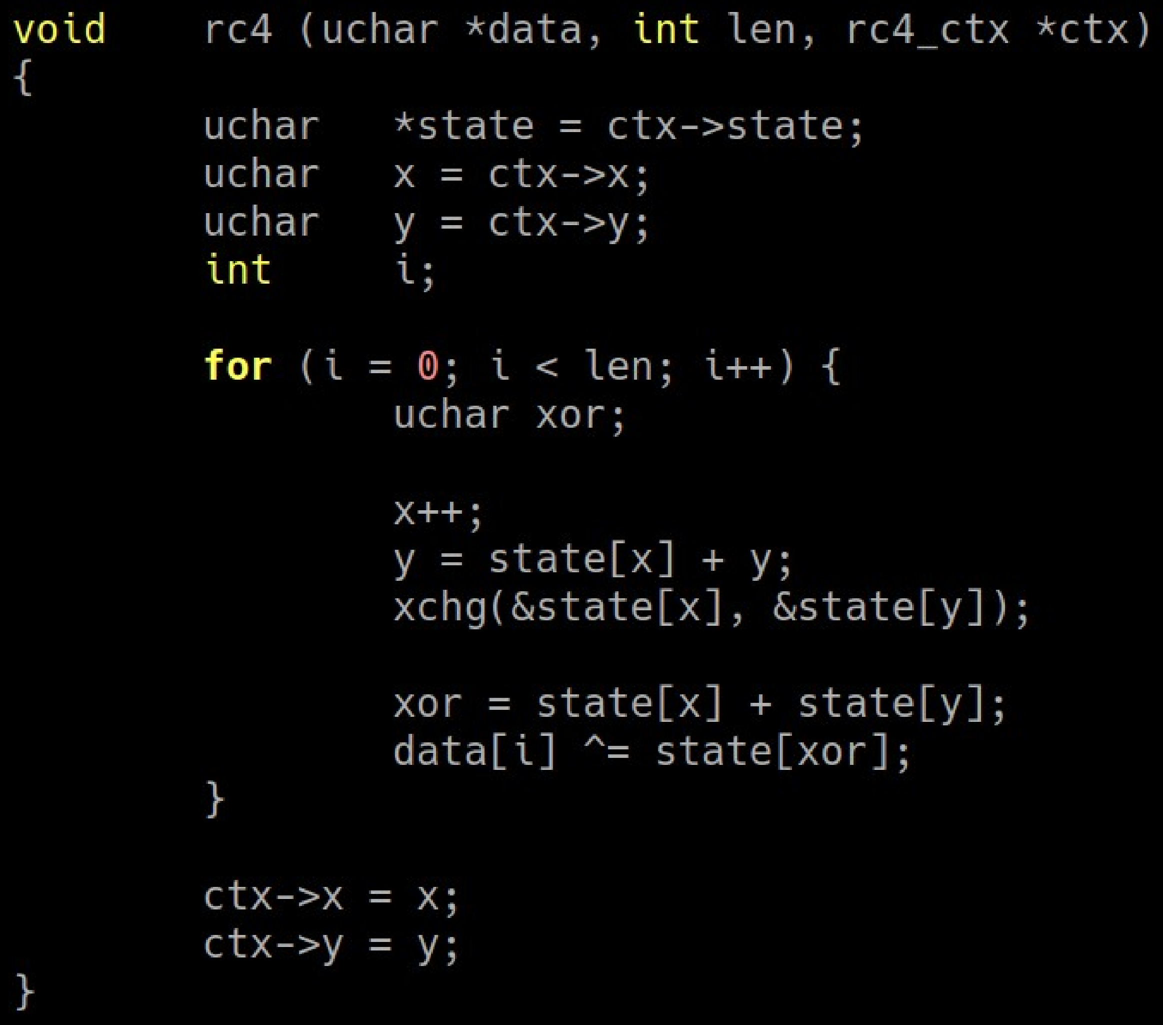


```
root@sandflysecurity:/proc/3306 # ls -al fd
total 0
dr-x------ 2 root root  0 Sep 11 23:32 .
dr-xr-xr-x 9 root root  0 Sep 11 23:29 ..
lrwx------ 1 root root 64 Sep 11 23:35 0 -> '/dev/pts/0 (deleted)'
lrwx------ 1 root root 64 Sep 11 23:35 1 -> '/dev/pts/0 (deleted)'
lrwx------ 1 root root 64 Sep 11 23:35 2 -> '/dev/pts/0 (deleted)'
lrwx------ 1 root root 64 Sep 11 23:35 3 -> 'socket:[32046]'
lrwx------ 1 root root 64 Sep 11 23:35 4 -> 'socket:[32057]'
root@sandflysecurity:/proc/3306 # grep 32057 /proc/net/*
grep: /proc/net/dev_snmp6: Is a directory
grep: /proc/net/netfilter: Is a directory
/proc/net/packet:ffff97ad4c31b000 3      3    0800   0     1 0      0      32057
grep: /proc/net/stat: Is a directory
root@sandflysecurity:/proc/3306 # 
```



Encrypted Comms

Encrypted Comms



```
void    rc4 (uchar *data, int len, rc4_ctx *ctx)
{
        uchar   *state = ctx->state;
        uchar   x = ctx->x;
        uchar   y = ctx->y;
        int     i;

        for (i = 0; i < len; i++) {
                uchar xor;

                x++;
                y = state[x] + y;
                xchg(&state[x], &state[y]);

                xor = state[x] + state[y];
                data[i] ^= state[xor];
        }

        ctx->x = x;
        ctx->y = y;
}
```

+ RC4 fast, small & secure enough.

- Will not match expected protocol on port.

Professional

SANDFLY SECURITY

“They have amongst them those who know very well what they are about…”

- Lord Percy on American Revolutionary War

Professional Malware

+ Fast and reliable.

+ Clever security bypasses.

+ Does not outsmart itself.

SANDFLY SECURITY

Closing Thoughts

SANDFLY SECURITY

Craig H. Rowland

@CraigHRowland
@SandflySecurity

www.sandflysecurity.com

https://sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/