Mastering Bash for Hackers: Extreme Command-Line Power

2026-10-22

Agenda (2h)

- about
- intro
- UNIX&CLI&bash
- cmdchallenge
- setup & 1st hands-on
- my snippets
- more hands-on

whoami

Founder and lead researcher at
Possible Security, Latvia
Mg. sc. comp., Mg. phys.

https://kirils.org/

Hobbies :)
Network flow analysis & RE

Kirils Solovjovs
bash expert

imagecrop-interactive

- My most recent ‘tool’ that I wrote Oct 2025
  - GIMP
  - vs gthumb
  - vs gthumb with keyboard shortcuts
  - vs imagemagick
  - vs imagecrop-interactive

imagecrop-interactive

- And of course, getting offsets for scripting!
  - Extracted images from a GoPro [..] but many images have weird artifacts [..] is there a fix somewhere?

Source: @richlv@mastodon.social

imagecrop-interactive

- ```
  for x in *.png; do
  convert $x  \(
   input.png -gravity east
  -crop 320x0+0+0 +repage \)
  -geometry +52+0
  -composite -gravity east
  -crop +52+0 +repage
  out-$x; done
  ```

Source: @richlv@mastodon.social
  ```

UNIX philosophy (ext., excerpt.)

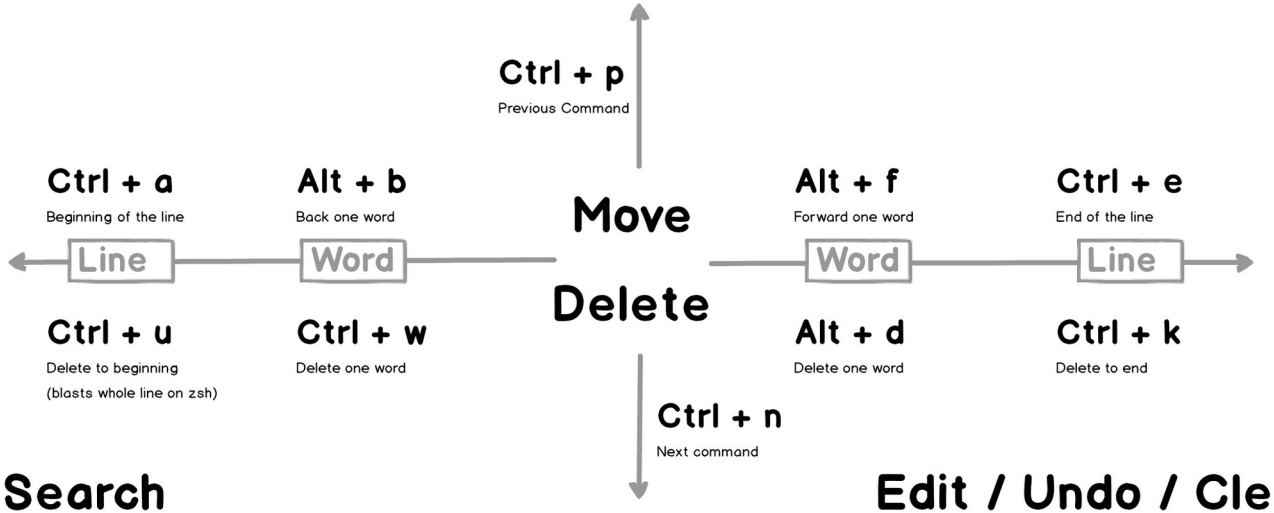
- Write programs that do one thing and do it well.
- Write programs to handle text streams, because that is a universal interface.
- Write programs to work together.
- When a program has nothing surprising to say, it should say nothing.

Source: https://cscie2x.dce.harvard.edu/hw/ch01s06.html

Bash

- Command Line **Interface**
- Installed by default on most UNIX systems
- Allows for networking, file system access, process control etc.

Typing @ prompt



Search

Ctrl + r Search Backwards

Ctrl + s Search Forwards

Ctrl + g Cancel

←, → Edit

Edit / Undo / Clear

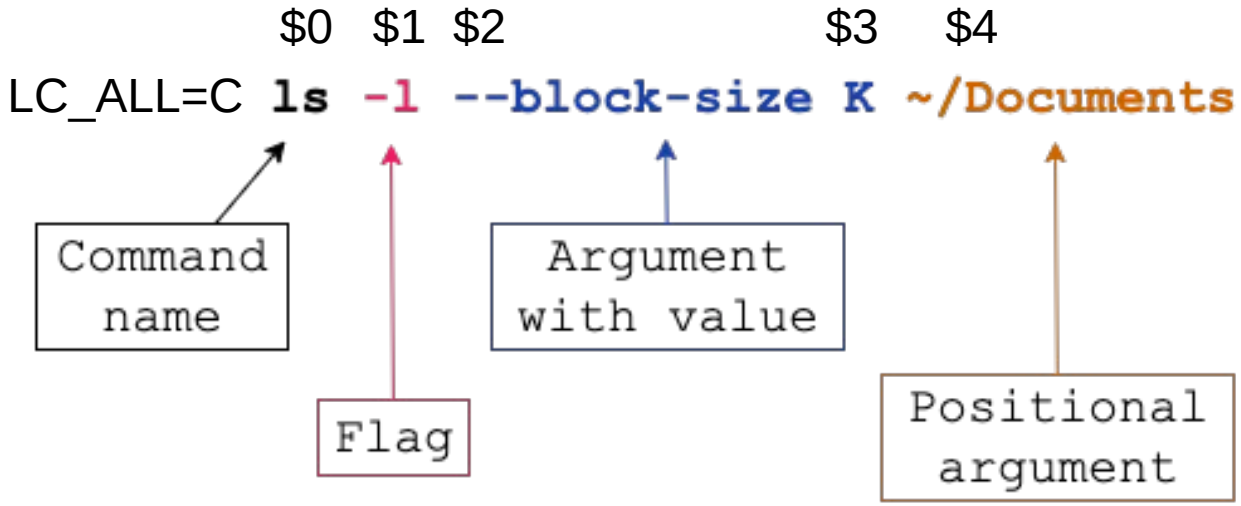
Ctrl + x,e Edit

Ctrl + l Clear

Cltr + - Undo

Credit: effective-shell.com

Command line



Credit: betterdev.blog

How is this organized

Starting off easy

- cmdchallenge.com

Clean machine

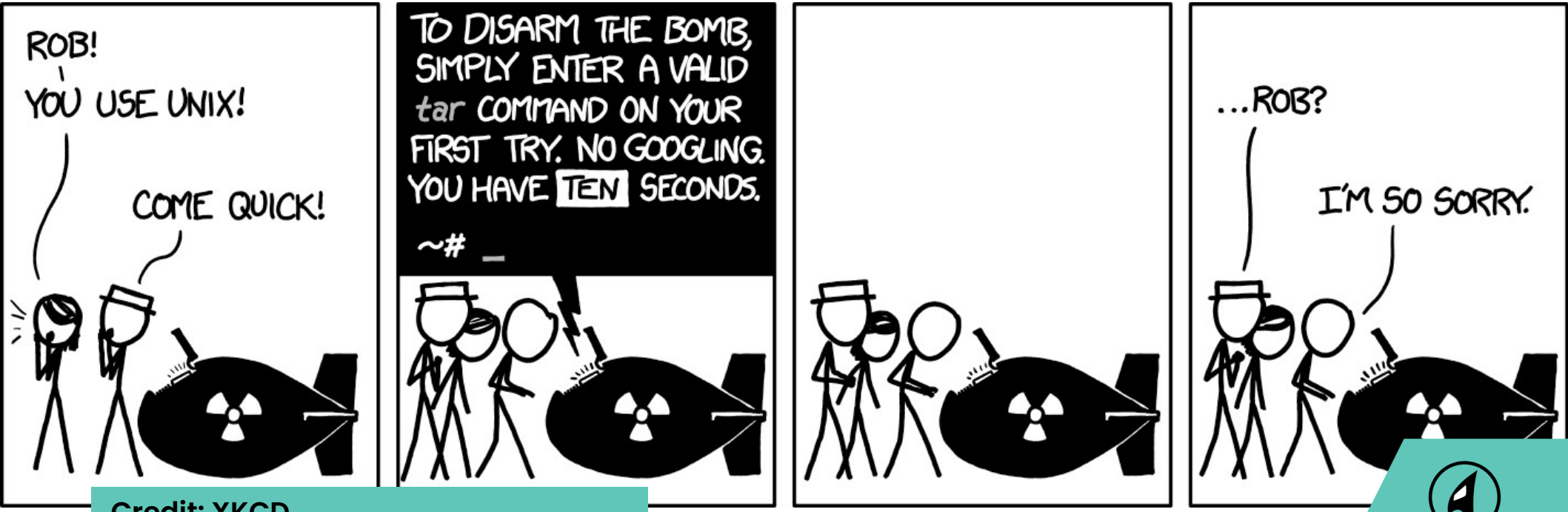
- packages:
  - progress
  - whois
  - php-cli
  - file
  - git
  - ??

Let’s play!

Download here

- https://github.com/0ki/shellscripts
- and here
  https://github.com/0ki/presentation-toolkit
- and here
  https://02.lv/f/2025/10/05/tasks_bash.tgz

Download here



Credit: XKCD

Task: access-A

- feel the file
- how many log entries?
- who is connecting?
- what response codes?

Task: tool exploration

- Explore presention-toolkit
  and shellscripts with me

Task: access-B

- look around
- how many log entries each day?
- most popular responses?
- most popular networks?
- graph networks against response codes

Task: data-A

- look around
- what categories did company #32 bid on?
- what are the average prices in those positions?
- who are the competitors in those positions?

Task: filesystem 1

- Find files modified in the last 5 days, and show how many of each filetype (magic) there are
  - ```
    find -mtime -5 -iname "*l*" | xargs file \
    | cut -d: -f2- |sed -E 's/^\s+//' |cut -d " " -f 1-2 \
    | sortuniq -c | sort -nr
    ```
  - ```
    find -mtime -5 -iname "*l*" | xargs file -b \
    | sortuniq -c | sort -nr
    ```
- Graph it
  - ```
    | chart countbar noheader noindex
    ```

    ```

# Task: filesystem 2

- Display modification date of files in this directory and all subdirectories

# That’s all folks!

Kirils Solovjovs
@k@chaos.social https://kirils.org/

possible.lv
IT security services
possible@possible.lv
+371 26036916