



possible.lv

IT security services

Mastering Bash for Hackers: Extreme Command-Line Power

BalCCon 2025-09-21



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



UNIX philosophy (ext., excerpt.)

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

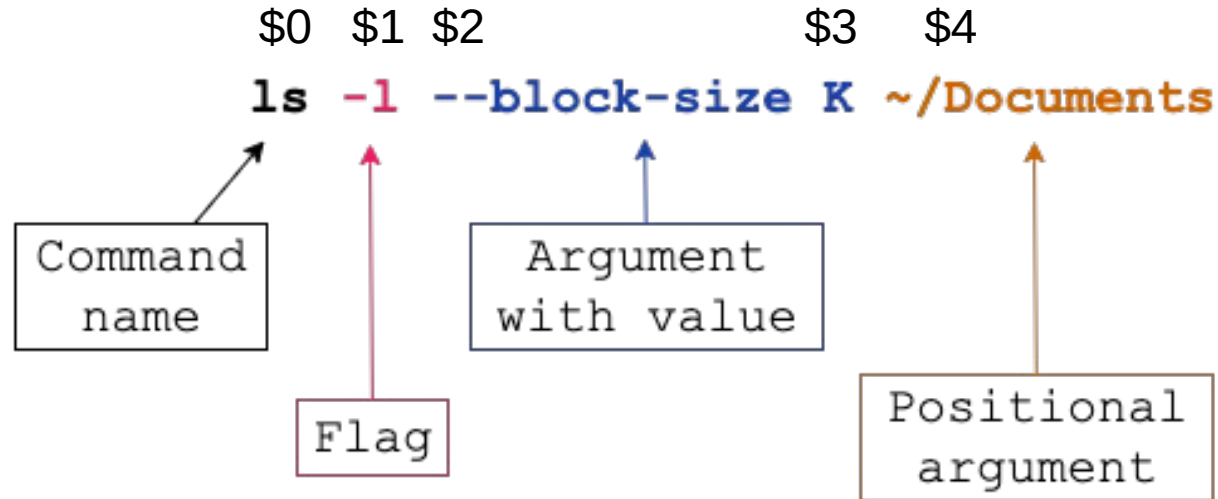


Bash

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



Command line



Credit: betterdev.blog



A person's hands are shown typing on a laptop keyboard and holding a smartphone. The image is overlaid with a teal banner containing the text "How is this organized". The background is a light blue and white color scheme with various digital icons and a network diagram.

How is this organized



Clean machine

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





Let's play!

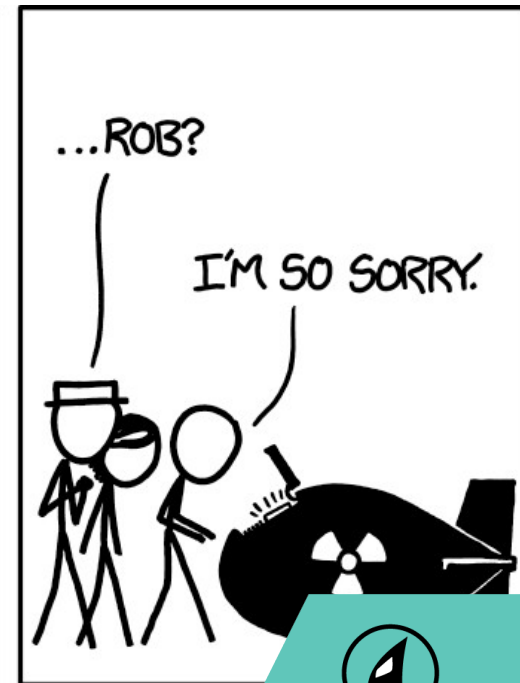
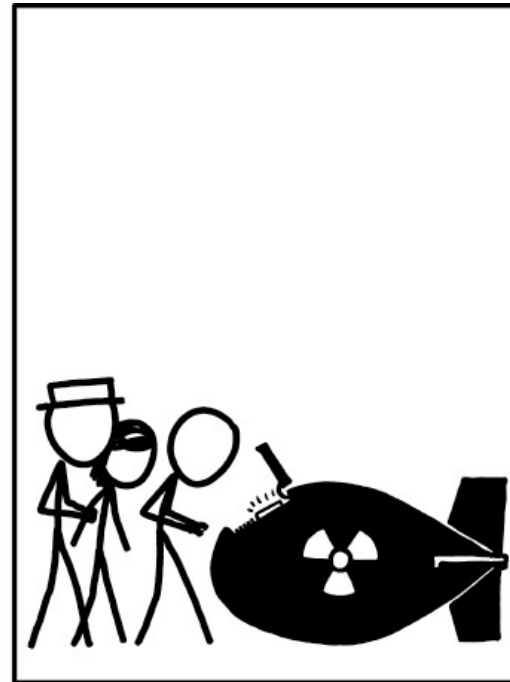
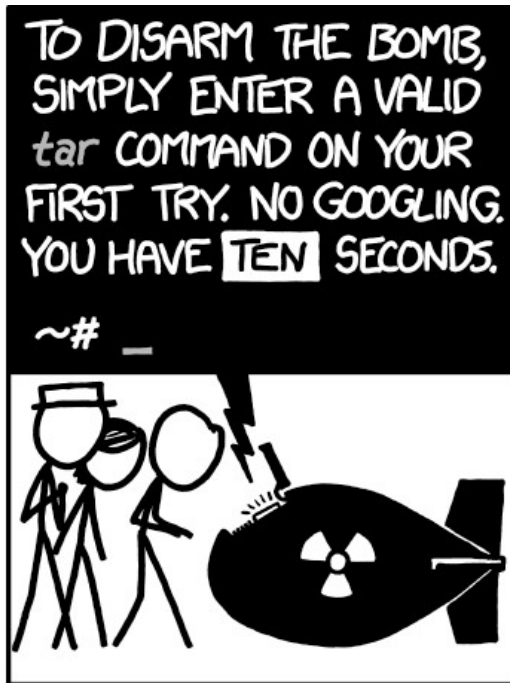


Download here

- https://02.lv/f/2025/09/18/tasks_bash.tgz
- and here
<https://github.com/0ki/shellscripts>
- and here
<https://github.com/0ki/presentation-toolkit>



Download here



Credit: XKCD



Task 0 - warmup

- Think about this:
 - trim a photo
 - convert a youtube video to still frames
- man pages!



Task 1 – access-A

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



Task 2 – access-B

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



Task 3 – 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 4 – filesystem 2

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



Task 5 - certificates

- Stream all the SSL certificates being issued for Serbian domains right now
- Hint:
 - `websocat | jq | grep`
- Answer:
 - `websocat wss://certstream.calidog.io/ \`
`| jq '.data.leaf_cert.subject.CN'|sed 's/./"https:\\/\\/' \`
`| grep rs\"`



Task 6 – tool exploration

- Explore presentation-toolkit and shellscripts with me





That's all folks!

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



possible.lv

IT security services

possible@possible.lv

+371 26036916