Security Nightmare for journalists
One day, we'll be all SysAdmin

Julie Gommes
@Jujusete

JOURNALISTS

what my friends think i do

what my mom thinks i do

what society thinks i do

what my editor thinks i do

what i think i do

what i actually do

In foreign country, you have to...

- Know tools you're using
- Connect to a distant server to put your datas
- Know how to connect in a safe way (like SSH) to put your datas on this server

- **And the Nightmare begins...**

Knowing your tools

- if you don't know how your computer works, you will not know how to crash/erase/cover traces of your datas
- If you don't use free software, how can you see what your devices are doing ?
- From Snowden files, when you buy a computer you don't know if NSA didn't put something inside

Having ~~fun~~ your own server

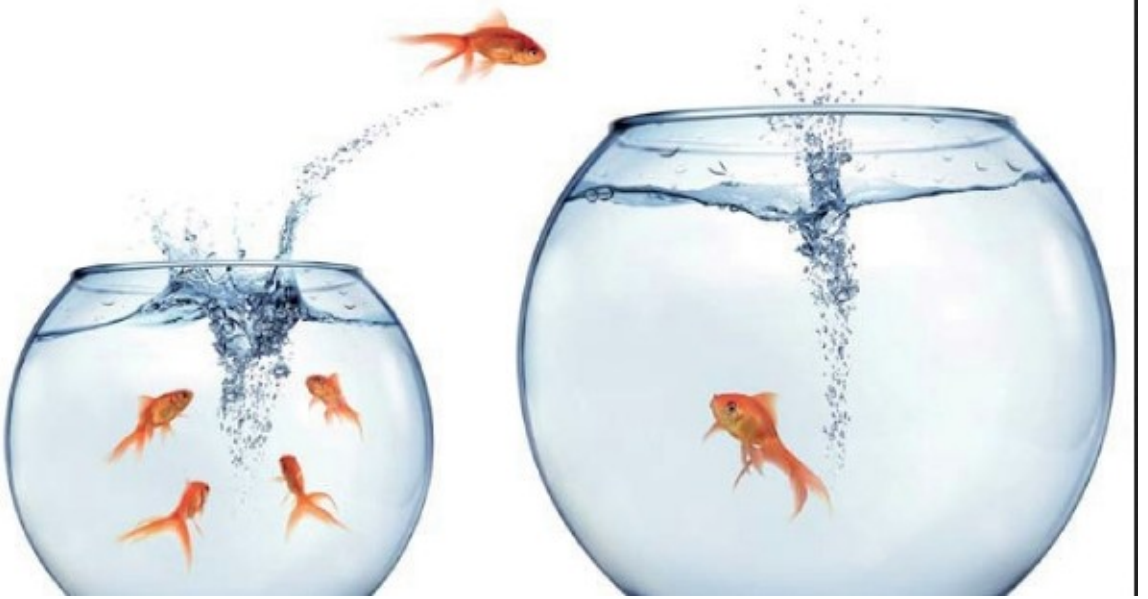
- Hosting at home or in a datacenter
  - Using command line to admin
  - Knowing about security
- On friend's server
  - settings for whether or not he/she has access to your space
  - good to start learning
- **If anyone can access to this server, datas are not protected**

Don't worry, this is only the beginning...

"I'm too tired to listen to a story tonight, dad. Just email it to me and I'll read it tomorrow."

transfer the data to the server

- Using Rsync
  - Using command line
  - Don't forget your .bash_history
- classical (s)FTP



Clear SD cards

- in SD cards, nothing is deleted physically before writing new things
- 'rm' data from the SD card: Danger!
  - Files are still there and any forensic software will be able to locate them
- Only effective protection: each time, cover the entire memory card randomly

dd if=/dev/urandom of=/dev/sdX bs=4M

Transfer datas

- Opening files before transfer is an other danger
  - software which is used for opening documents keep an history of opened files
- Pictures and sounds files also contain metadata: moment of recording, GPS position, model of the device...
  - **So you have to kill all of that**
  - **https://wiki.archlinux.org/index.php/Securely_wipe_disk**

.bash_history

- Command 'rsync' transfer datas remain in user's .bash_history
- You have to modify your .bash_history to don't keep memories of Rsync

  http://www.techrepublic.com/article/linux-command-line-tips-history-and-histignore-in-bash/

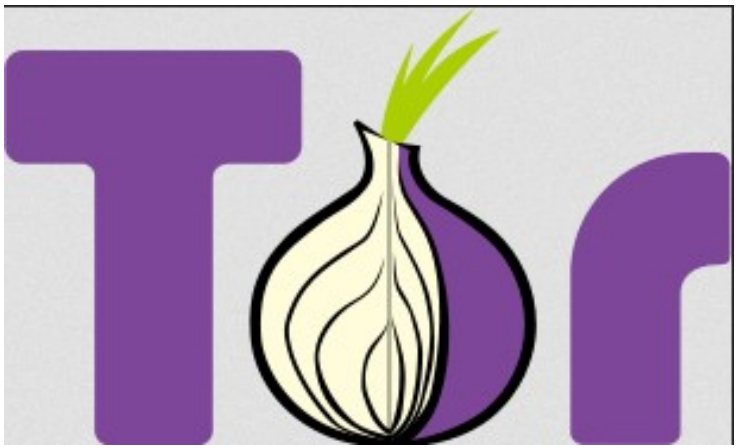
Server security

- Connect via SSH
- encrypted folders in other encrypted folders, in encrypted disk in...
- Not hosting stuff you don't know security level
- check folder permissions

- who has access to the server?

When a nightmare can be a dream

Using Tails



- each time you need transfer datas
- Nothing on the hard disk
- Connection will be through Tor
- Rsync is in tails

Outro...
(for an other night...)

Login SSH server through Tor ?

- Using private key or Passphrase ?
- Store the private key on an encrypted flash key (using LUKS)
- Mount your flasjkey from the live distro.
- Can it become more complex than manage an authentication passphrase ?

Thank you !
Questions ?