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

Julie Gommes
@Jujusete

Irc : Jujusete on Freenode, Geeknode, europnet, oftc...

DefCamp14, Bucarest

Who am I ?

- Padawan talking to his computer with feet using command line
- Journalist during 12 years, 4 years in lovely countries like Egypt, Sudan, Syria, Vetnam, Thaïland...
- I love to collect 56k modems and not just for the noise
- I also participate to non profit provider

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...**

In France too ?

- New law project against « terrorism »
- To find those people they have to monitor what we're all doing
- So if you're journalist, they can see all you're doing online, so they can know who are your sources...
- 1886 : attempt in Paris (La Bourse) – fail
- Lqdn = http://presumes-terroristes.fr/

Knowing your tools

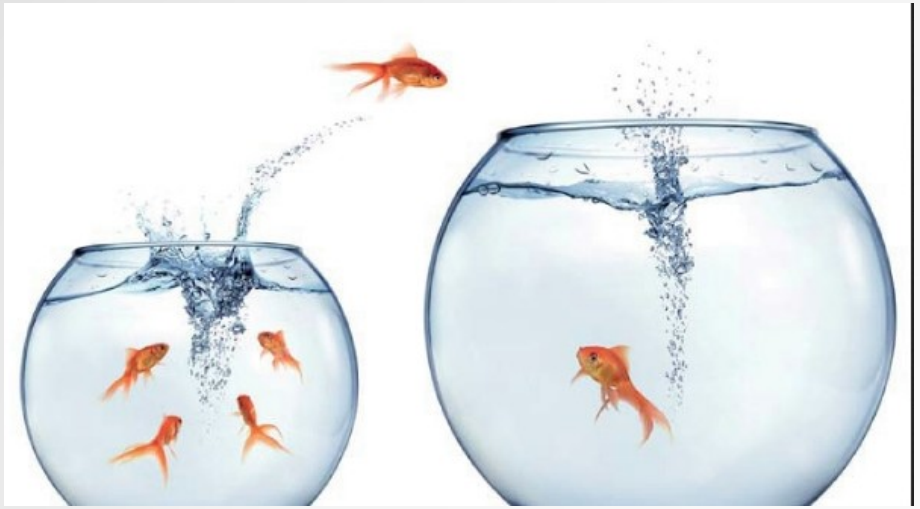
- if you don't know how your computer works, you will not know how to crash/erase/cover traks of your datas
- If you don't use free software, how can you see what your devices are doing ?
- From Snowden files, when you buy a computer you don't know if NSA didn't put something inside

Havin ~~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 just the first steps...

transfer the data to the server



- **Using Rsync**
  - Using command line
  - Don't forget your .bash_history

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

- rsync -axv --progress /home/machine/DossierDenvoi/ truc@serveur.xx:DossierDeReception/

.bash_histowhat ?

WIKIPÉDIA
L'encyclopédie libre

Article | Discussion | Lire | Modifier | Modifier le code

Bourne-Again shell

Ne doit pas être confondu avec batch ni bâche.

Bash, acronyme de ***Bourne-Again shell***, est le shell du projet GNU. Son nom est un jeu de mots sur le nom du *shell* historique d'Unix, le Bourne shell. Littéralement, *Bourne again* signifie « Bourne encore », mais se prononce également presque comme *born again*, signifiant « né de nouveau » ou encore « réincarné ». Également, *to bash* signifie « frapper violemment » en anglais.

Basé sur le Bourne shell, Bash lui apporte de nombreuses améliorations, provenant notamment du Korn shell et du C shell. Bash est un logiciel libre publié sous GNU GPL. Il est l'interprète par défaut sur de nombreux Unix libres, notamment sur les systèmes GNU/Linux. C'est aussi le shell par défaut de Mac OS X et il a été porté sous Windows par le projet Cygwin.

- https://fr.wikipedia.org/wiki/Bourne-Again_shell

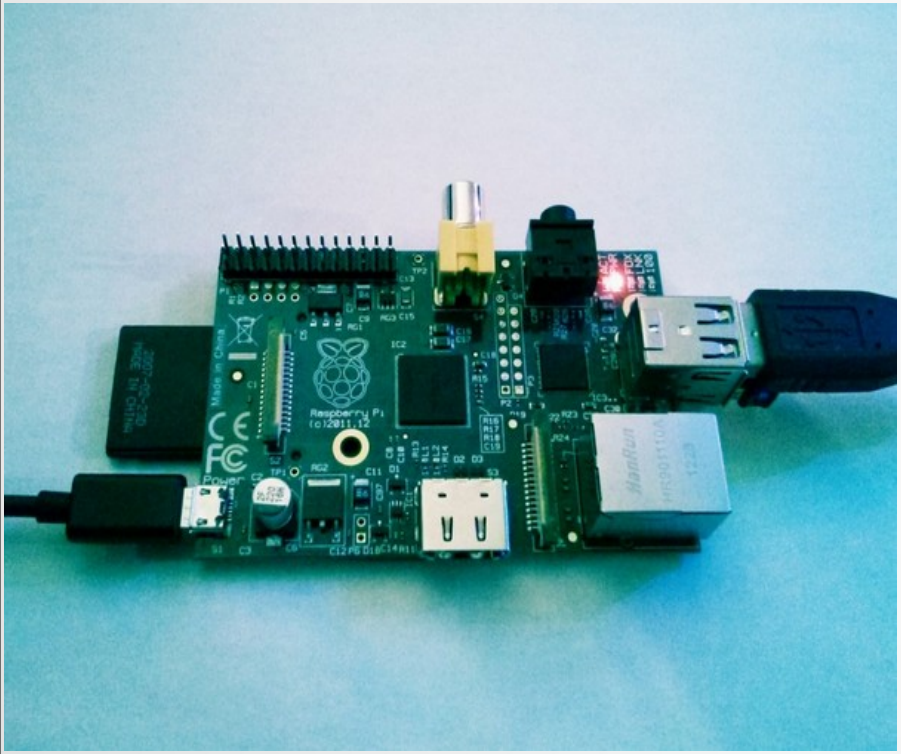
Clear SD cards

- 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/sd(n°) 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**



- Never plug on your computer without checking security stuff
- Using RasPi to mount/create an iso/verify if PDF aren't hidden .exe

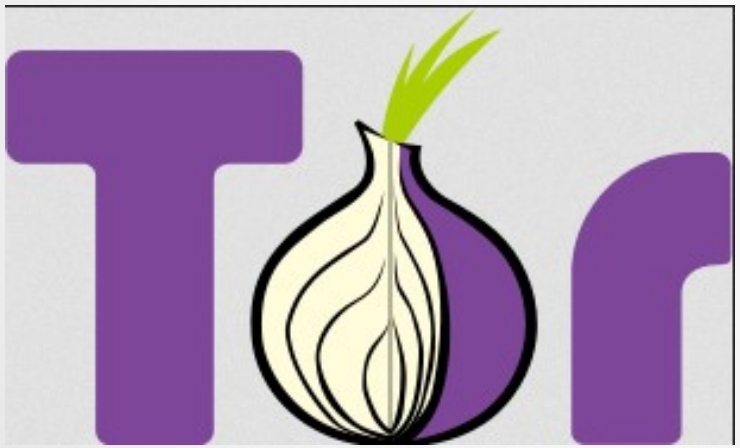
Server security

- 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 server through Tor ?

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

Thank you ! Questions ?