ANNEX A · SUDO AND LEAST PRIVILEGE

Name: _____ **Date:** _____

Work in `deb-lab`. Users marta, joan, aina, pau have the lab passphrase `quatre gats negres dormen`. **Safety net:** open a second terminal, run `sudo -i` there and leave it open until the end.

TASK 1 **What may you do?**

Run `sudo -l`. Copy the last line: _____
Run `sudo grep -vE "^#|^$" /etc/sudoers`. Which line gives you that power?

_____

TASK 2 **What may marta do?**

Run `su - marta`, then `sudo whoami`. Answer: _____
Type `exit`.
DONE WHEN the prompt shows your own user again.

TASK 3 **Write the rules of Tramuntana Apps.**

The intern may refresh the package lists and nothing else. The dev team may restart the scheduler.

```
sudo visudo -f /etc/sudoers.d/tramuntana
```

Type these three lines, save (`Ctrl + O`, Enter) and leave (`Ctrl + X`). If it says `What now?`, answer `e` and fix the line.

```
# Tramuntana Apps - least privilege
pau   ALL=(root) /usr/bin/apt update
%dev  ALL=(root) /usr/bin/systemctl restart cron
```

DONE WHEN `sudo visudo -c` prints `parsed OK` for every file.

TASK 4 **Test as the intern.**

Run `su - pau`. Then, as pau:

`sudo -l` — which commands are listed?

_____

`sudo apt update` — does it work? _____
`sudo apt install cowsay` — what does it answer?

_____

`sudo whoami` — _____
Why does pau have **two** commands when you wrote only one line with his name?

_____

Type `exit`.

TASK 5 **Check the others without becoming them.**

`sudo -l -U joan` → _____

`sudo -l -U marta` → _____

TASK 6 **Who did what?**

Run `sudo journalctl -t sudo -n 10`. Find the line of pau's refused command. Which words say it was refused? _____

TASK 7 **Think before you grant.**

The boss asks: "Aina should be able to create accounts for new employees." Someone proposes this rule:

```
aina  ALL=(root) /usr/sbin/adduser
```

With only this rule, how could aina become a full administrator? Write the command she would run. (Do not add the rule.)

EXIT TICKET **Alone, no terminal. Tick one answer.**

1. In `%dev ALL=(root) /usr/bin/systemctl restart cron`, what does `%` mean?

- ☐ a) a comment
- ☐ b) `dev` is a group
- ☐ c) `dev` is a machine
- ☐ d) no password is asked

2. Why edit the rules with `visudo` and not directly with `nano`?

- ☐ a) `nano` cannot open that folder
- ☐ b) `visudo` asks for no password
- ☐ c) `visudo` is faster
- ☐ d) `visudo` checks the grammar before saving

3. The principle of least privilege says:

- ☐ a) give each account only what its job needs
- ☐ b) give nobody any rights
- ☐ c) give everybody `sudo`, with a log
- ☐ d) change passwords every month

4. Joan must restart the print service `cups` from time to time. Which is the best solution?

- ☐ a) add joan to the group `sudo`
- ☐ b) tell joan root's password
- ☐ c) `joan ALL=(root) /usr/bin/systemctl restart cups`
- ☐ d) `joan ALL=(ALL:ALL) ALL`