ANNEX A · ACCOUNT AND PASSWORD POLICIES

Name: _____ **Date:** _____

PART A **Look inside `/etc/shadow` (15 min).** In `deb-lab`.

A1 Run `sudo grep "^marta:" /etc/shadow`. First three characters of field 2: _____ Field 3 (a number): _____

Turn it into a date: `date -d "1970-01-01 +N days" +%F` (N = your number): _____

A2 Run `echo -n tramuntana | sha256sum` and `echo -n tramuntanA | sha256sum`. First four characters of each: _____

A3 Run `openssl passwd -6 tramuntana` twice. Same result? _____ Now twice with `-salt abcdefgh` before the password. Same? _____

A4 Marta and joan have the same password. Compare field 2 of their lines in `/etc/shadow`. Same? _____ Why? _____

A5 Run `sudo chage -l marta`. Password expires: _____ Maximum days: _____

DONE WHEN you can explain to your neighbour why root cannot read marta's password.

PRACTICAL 5.3 **A password policy for Tramuntana Apps (40 min).**

Before you start: in virt-manager take a snapshot of `deb-lab` called `before-pam`. Open a **second terminal**, run `sudo -i` in it and do not close it: it is your way back in.

TASK 1 **Accounts: the intern's contract ends on 30 June; marta's password is known to everybody.**

```
sudo chage -E 2027-06-30 pau
sudo chage -d 0 marta
sudo chage -l pau
sudo chage -l marta
```

DONE WHEN pau shows `Account expires : Jun 30, 2027` and marta shows `password must be changed`.

TASK 2 **Quality: at least 15 characters, no obvious passwords.**

Run `sudo apt install libpam-pwquality`. Then `sudo nano /etc/security/pwquality.conf`: find the line `# minlen = 8` and change it to `minlen = 15` (no `#`).

DONE WHEN `grep pwquality /etc/pam.d/common-password` prints a line, and `grep "^minlen" /etc/security/pwquality.conf` prints `minlen = 15`.

TASK 3 **Test it as marta: `su - marta` (old password `tramuntana`). Try these new passwords, in this order.**

`Tr4mun!` → _____

`123456789012345` → _____

`quatre gats negres dormen` → _____

Type `exit`. Now, as administrator, run `sudo passwd pau` and try `1234`. What is different?

_____

Give pau, joan and aina the lab passphrase `quatre gats negres dormen` with `sudo passwd`.

DONE WHEN `su - marta` accepts the passphrase and refuses `tramuntana`.

TASK 4 **Lockout on Linux — only if it is before 1:20; if not, watch the demo. Three wrong guesses lock the account for 10 minutes.**

`sudo nano /etc/pam.d/common-auth`. Change and add lines until the lines without `#` read like this (leave any other line where it is):

```
auth  required                    pam_faillock.so preauth          new line
auth  [success=2 default=ignore]  pam_unix.so nullok               was success=1
auth  [default=die]               pam_faillock.so authfail         new line
auth  requisite                   pam_deny.so                      (already there)
auth  sufficient                  pam_faillock.so authsucc         new line
auth  required                    pam_permit.so                    (already there)
```

`sudo nano /etc/pam.d/common-account`: add, above the first line that starts with `account`:

`account  required  pam_faillock.so`

`sudo nano /etc/security/faillock.conf`: remove the `#` of `deny = 3` and of `unlock_time = 600`.

Test: `su - joan` with a wrong password, three times. Then with the right one. Message:

`sudo faillock --user joan` — how many lines? _____ Unlock: `sudo faillock --user joan --reset`

DONE WHEN after the reset, `su - joan` works again with the right passphrase. Your own `sudo` still works.

TASK 5 Windows: the same policy in `win11`, in Terminal (Admin).

Run `net accounts`. Minimum password length: _____ Maximum password age: _____ Lockout threshold: _____

```
net accounts /minpwlen:14 /maxpwage:unlimited /lockoutthreshold:5
net accounts
net user marta *
```

Give marta a 5-character password. Answer: _____

Why 14 and not 15? Try `/minpwlen:15` and read the error. _____

DONE WHEN `net accounts` shows 14, Unlimited and 5.

HAND IN `practical-5.3-surname.md` on Classroom by **Thursday 04/03, 23:59**: commands and outputs of each task, and a table "setting → reason" with one line per rule you set (why 15? why no expiry? why lockout?). Marking (10): task 1: 2 · tasks 2–3: 3 · task 4: 1.5 · task 5: 1.5 · reasons: 1.5 · report: 0.5. Never write a real password of yours in a report.

EXIT TICKET Alone, no terminal. Tick one answer.

1. What does `/etc/shadow` keep for each user?

- ☐ a) the password
- ☐ b) the password, encrypted with root's key
- ☐ c) a salted hash of the password
- ☐ d) nothing about passwords

2. What is the salt for?

- ☐ a) equal passwords give different hashes
- ☐ b) it makes the password longer to type
- ☐ c) it lets root read the password
- ☐ d) it compresses the file

3. What does NIST say today about changing passwords?

- ☐ a) every 30 days
- ☐ b) every 90 days
- ☐ c) once a year
- ☐ d) only when there is evidence of compromise

4. Which password is the hardest to guess?

- ☐ a) `Tr4mun!`
- ☐ b) `quatre gats negres dormen`
- ☐ c) `P@ssw0rd1`
- ☐ d) `123456789012345`

5. Laia's internship ends on 31 March. Which command makes her account stop working that day?

- ☐ a) `sudo chage -E 2027-03-31 laia`
- ☐ b) `sudo chage -d 0 laia`
- ☐ c) `sudo passwd -S laia`
- ☐ d) `sudo usermod -aG dev laia`