ANNEX A · USER RIGHTS AND SECURITY POLICIES

Name: _____ **Date:** _____

0 · Safety first. In virt-manager take a snapshot called `before-rights` of `win11` **and** of `ubu-srv`.

LAB A · WINDOWS: THE LOCAL SECURITY POLICY (ON `WIN11`, SIGNED IN AS ADMINISTRATOR)

1 · My own rights. Open a terminal and run `whoami /priv`. Then open a terminal **as administrator** and run it again.

☐ **Done when:** you counted the privileges. Normal terminal: _____ Administrator terminal: _____

2 · Read the policy. Start → type `secpol.msc` → Enter. Open Local Policies → User Rights Assignment. Who has each right?

User right	Accounts and groups on your PC
Allow log on locally	
Allow log on through Remote Desktop Services	
Shut down the system	
Change the system time	

☐ **Done when:** the table is full. Which of the four explains what we had to do on 16/04 for remote desktop?

_____

3 · Change a right and test it. Administrator terminal: `net user pau Benvinguda-2027 /add`. In `secpol.msc`: Deny log on locally → Add User or Group → `pau` → OK. Sign out and try to sign in as `pau`. Then sign in as administrator, remove `pau` from the policy, and try again.

☐ **Done when:** `pau` was refused the first time and got in the second time. `pau` is also in Users, which is allowed to log on locally. Which list wins? _____

4 · A security option. Local Policies → Security Options. Set Interactive logon: Message title for users attempting to log on to `Tramuntana Apps` and Interactive logon: Message text for users attempting to log on to `Authorised staff only. Activity on this computer is logged.` Sign out.

☐ **Done when:** the notice appears before the sign-in screen.

5 · The policy as a text file. Administrator terminal:

```
secedit /export /cfg C:\policy.inf /areas USER_RIGHTS
notepad C:\policy.inf
```

☐ **Done when:** you found the line that starts with `SeShutdownPrivilege`. What do you think `Se...Privilege` lines are? _____

LAB B · LINUX: AUDIT AND RIGHTS BY DEPARTMENT (ON `UBU-SRV`, `SSH SRV`)

Keep a second SSH session to `ubu-srv` open in another terminal until the end.

6 · The audit: who is root on this server? On 14/04 you closed a hole: Ubuntu made the group `admin` root. Is it still closed?

```
sudo grep -n admin /etc/sudoers
getent group sudo
for u in marta pau joan aina; do sudo -l -U $u; done
```

The `%admin` line starts with: _____ Members of the group `sudo`: _____ Can aina use sudo? _____

If aina can: `sudo visudo`, put a `#` at the start of the line `%admin ALL=(ALL) ALL`, save.

☐ **Done when:** the only account that can become root is yours, and you can show the three outputs that prove it.

7 · One task per department. `sudo visudo -f /etc/sudoers.d/tramuntana` and write:

```
# Tramuntana Apps: rights by department
%dev     ALL=(root) /usr/bin/systemctl restart smbd, /usr/bin/journalctl -u smbd
%design  ALL=(root) /usr/bin/systemctl restart cups
```

```
sudo -l -U marta
sudo -l -U joan
sudo -i -u marta
sudo cat /etc/shadow
sudo journalctl -u smbd -n 5
exit
```

☐ **Done when:** `sudo -l` shows the right commands for each one, and marta was refused twice. Why was the second one refused? _____

8 · Who may log in over SSH. Give marta and joan your own key, so that you can test:

```
for u in marta joan; do sudo mkdir -p /home/$u/.ssh; sudo cp ~/.ssh/authorized_keys /home/$u/.ssh/; sudo chown -R $u: /home/$u/.ssh; done
```

From your host, check that `ssh marta@192.168.122.10` and `ssh joan@192.168.122.10` both work. Then, on `ubu-srv`, add these four lines at the **end** of `/etc/security/access.conf` (`sudo nano`):

```
+:root:ALL
+:(sudo):ALL
+:(dev) (admin):ALL
-:ALL:ALL
```

In `/etc/pam.d/sshd` (`sudo nano`), find the line `# account required pam_access.so` and delete only the `#`.

☐ **Done when:** from the host, marta gets a shell, joan gets `Connection closed`, and **you** can still log in. Which line lets you in? _____

9 · A limit (if you have time). Add the line `@dev hard nproc 200` at the end of `/etc/security/limits.conf`.

☐ **Done when:** `ssh marta@192.168.122.10 'ulimit -u'` prints `200`.

10 · Log it. Add today's entry to `~/server-log.md` and tick line 9 of the project checklist.

EXIT TICKET

☐ **1.** "Pau may not log in to this PC." What kind of rule is that?
A) A file permission B) A user right C) A share permission D) A password policy

☐ **2.** Where does Windows keep the list of who may shut down the system?
A) In the folder's Security tab B) In Task Manager C) In Disk Management
D) In the Local Security Policy, under User Rights Assignment

☐ **3.** An account is in "Allow log on locally" and in "Deny log on locally". Result?
A) It cannot log on B) It can log on C) Windows asks the administrator D) An error at boot

☐ **4.** What does `%dev ALL=(root) /usr/bin/systemctl restart smbd` allow?
A) The user `dev` to run any command B) Everybody to restart Samba
C) The group `dev` to run exactly that command as root D) The group `dev` to become root

☐ **5.** Which file does `pam_access` read to decide who may log in?
A) `/etc/passwd` B) `/etc/security/access.conf` C) `/etc/sudoers` D) `/etc/fstab`