ANNEX A · PRACTICAL 6.1 — SSH WITH KEYS

Name: _____ **Date:** _____ **Group:** DAM-1

Client: `deb-lab`. Server: `ubu-srv`. **YOU** = your user name on `ubu-srv`. Take a snapshot `pre-ssh` of `ubu-srv` first.

TASK 1 First connection: check who you are talking to

On the **console** of `ubu-srv` (the virt-manager window):

```
ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub
```

Last 6 characters of the `SHA256:` fingerprint: _____

On `deb-lab`: `ssh YOU@ubu-srv`. Compare the fingerprint it shows. Same? _____ Then type `yes`, log in, and `exit`.

☐ **DONE WHEN** the two fingerprints are the same and you logged in with your password.

TASK 2 Make your key pair

On `deb-lab`. Accept the file name. **Type a passphrase** when it asks.

```
ssh-keygen -t ed25519 -C "YOU@deb-lab"
ls -l ~/.ssh
```

Which file is the secret one? _____ Its permissions: _____

☐ **DONE WHEN** `~/.ssh` has `id_ed25519` and `id_ed25519.pub`.

TASK 3 Hang your padlock on the server

```
ssh-copy-id YOU@ubu-srv
ssh YOU@ubu-srv
cat ~/.ssh/authorized_keys
exit
```

What did the login ask for this time? _____

☐ **DONE WHEN** you log in without typing the **server** password, and `authorized_keys` has one line.

TASK 4 A short name

On `deb-lab`, create `~/.ssh/config` with `nano`:

```
Host srv
    HostName ubu-srv
    User YOU
    IdentityFile ~/.ssh/id_ed25519
```

```
chmod 600 ~/.ssh/config
ssh srv hostname
```

☐ **DONE WHEN** `ssh srv hostname` prints `ubu-srv`.

TASK 5 Files in both directions

```
echo "hello from deb-lab" > notes.txt
mkdir project && touch project/a project/b
scp notes.txt srv:
scp -r project srv:
scp srv:/etc/hostname server-name.txt
ssh srv ls
```

What does `ssh srv ls` show? _____

☐ **DONE WHEN** `notes.txt` and `project` are on the server, and `server-name.txt` is on `deb-lab`.

TASK 6 Keys only

Open a second terminal, run `ssh srv` in it and leave it open until the end. In the first one:

```
ssh -o PubkeyAuthentication=no srv        # before: what does it ask?
ssh srv
sudo nano /etc/ssh/sshd_config.d/10-tramuntana.conf
```

Write these three lines in the file:

```
PasswordAuthentication no
KbdInteractiveAuthentication no
PermitRootLogin no
```

```
sudo sshd -t                              # no output = no mistakes
sudo systemctl restart ssh
exit
ssh -o PubkeyAuthentication=no srv        # after: what does it say?
ssh srv hostname
```

Before: _____ After: _____

☐ **DONE WHEN** without the key you get **`Permission denied (publickey).`** and with the key you still get in.

TASK 7 Read the log

```
ssh srv
sudo journalctl -u ssh -n 20
```

Find your refused attempt. From which address did it come? _____ At what time?

_____

TASK 8 A server on the Internet

Paste the content of **`~/.ssh/id_ed25519.pub`** (one line, starts with **`ssh-ed25519`**) in the Classroom assignment. Never the file without **`.pub`**. When the teacher says "go", connect to the address on the board:

```
ssh YOU@ADDRESS-ON-THE-BOARD
```

☐ **DONE WHEN** you are in a shell on the online server and never typed a password for it.

Hand in on Classroom: **`practical-6.1-surname.md`** with, for each task, the command and its output (copy the text, no photos) and one sentence saying what it proves. **Marking (10):** fingerprint compared 1 · key pair with passphrase 1.5 · login with the key 2 · alias 1 · **`scp`** both ways 1 · passwords and root login off, shown with the test 2 · log line found 1 · clear report 0.5.

Exit ticket — alone, no notes. One answer each.

1. Which file do you put on the server?

☐ **a)** **`id_ed25519`** ☐ **b)** **`known_hosts`**
☐ **c)** The content of **`id_ed25519.pub`** ☐ **d)** **`config`**

2. The first time you connect, **`ssh`** shows a fingerprint. What is it for?

☐ **a)** To choose the encryption ☐ **b)** To check the server is the real one
☐ **c)** To check your password is strong ☐ **d)** To create your key pair

3. **`scp notes.txt srv`** — what happens?

☐ **a)** The file goes to the server's home ☐ **b)** The file goes to **`/tmp`** on the server
☐ **c)** An error: no such host ☐ **d)** A local copy named **`srv`** is made

4. What do you do before you restart SSH with a new configuration?

☐ **a)** Keep one SSH session open ☐ **b)** Close every session
☐ **c)** Delete **`authorized_keys`** ☐ **d)** Reboot the client