ANNEX A · LOGS & JOURNALD · WORKSHEET

Name: _____ **Date:** _____ **Group:** _____

Work in `deb-lab` (tasks 1–9) and `win11` (tasks 10–12). Leave the pager with `q`. Write what **your** machine shows.

PART A · ASK THE JOURNAL

Task 1 · Who may read? Run both and compare.

```
journalctl -n 5
sudo journalctl -n 5
```

Without `sudo`, the hint says you are not seeing: _____

Task 2 · Write a line and watch it arrive. Open two terminals. In the first: `sudo journalctl -f`. In the second:

```
logger -t tramuntana "hello from YOUR-NAME"
```

Copy your line from the first terminal: _____

Its four parts: when _____ host _____ who _____ what _____

DONE WHEN your message appeared without you pressing anything in the first terminal. Leave it with `Ctrl+C`.

Task 3 · One service.

```
sudo journalctl -u heartbeat -n 5
sudo journalctl -u heartbeat --since today | wc -l
```

Lines written by `heartbeat` today: _____ Roughly how many per minute? _____

Task 4 · Time windows. Write the command that shows…

the journal of this boot only: _____

the last 10 minutes: _____

How many boots does `sudo journalctl --list-boots` list? _____

Task 5 · How bad? Send an error on purpose, then filter by priority.

```
sudo journalctl -p err -b
logger -p user.err -t tramuntana "disk almost full (test)"
sudo journalctl -t tramuntana -p err
```

Lines of level `err` or worse in this boot: _____ Does the last command show your “hello” of task 2? _____

Why (not)? _____

DONE WHEN you can say which number is worse, 3 or 6.

PART B · THE LOG HUNT

Task 6 · Yesterday’s crime. Yesterday you killed your heartbeat service with `kill -9`. Find the line.

```
sudo journalctl -u heartbeat --since yesterday -g "killed|restart"
```

Exact time: _____ Signal (`status=`): _____ Who wrote the line? _____

Why was it not `heartbeat.sh` that wrote it? _____

DONE WHEN you have the second in which your service died.

Task 7 · A failed sudo. Type a **wrong** password three times, then the right one.

```
sudo -k
sudo ls /root
sudo journalctl -t sudo --since "5 min ago"
```

From the line with “incorrect password”: user _____ attempts _____ `PWD=` _____ `COMMAND=` _____

Is a **successful** `sudo` also written down? _____

Task 8 · Reboots. `sudo journalctl --list-boots` — first entry of boot 0: _____

Task 9 · What was installed? Some programs still keep text files.

```
grep -A1 "Start-Date" /var/log/apt/history.log | tail -4
ls /var/log/syslog
```

Last `apt` command recorded: _____ Date: _____

`ls /var/log/syslog` says: _____

DONE WHEN you found the date of an install you did this month.

PART C · WINDOWS

Task 10 · Errors. `Win+R` → `eventvwr.msc` → Windows Logs → **System** → **Filter Current Log…** → tick **Critical** and **Error**.

Events shown: _____ Newest one — date: _____ Source: _____ Event ID: _____

Task 11 · Services. Same log. Filter by **Event sources** = **Service Control Manager**. Open one event.

Event IDs you see: _____ Text of one of them: _____

Task 12 · Logons. PowerShell as administrator. Then fail one logon on purpose and find it.

```
Get-WinEvent -FilterHashtable @{ LogName='Security'; Id=4624 } -MaxEvents 3
runas /user:pau cmd
Get-WinEvent -FilterHashtable @{ LogName='Security'; Id=4625 } -MaxEvents 1
```

Time of the newest successful logon: _____ Time of the failed one: _____

DONE WHEN you found your own failed logon by its number.

EXIT TICKET (NO VM, ALONE)

1. Which command shows only the lines of the service `heartbeat`?

☐ **a)** `journalctl -p heartbeat` ☐ **b)** `journalctl -u heartbeat`

☐ **c)** `journalctl -f heartbeat` ☐ **d)** `journalctl -b heartbeat`

2. What does `journalctl -p err` show?

☐ **a)** Only priority 3 ☐ **b)** Priorities 3 to 7

☐ **c)** Only lines with the word “error” ☐ **d)** Priority 3 and everything worse (0–3)

3. You want to watch new log lines appear while you test something. Which option?

☐ **a)** `-f` ☐ **b)** `-n` ☐ **c)** `-b` ☐ **d)** `-r`

4. On Debian 13, where are yesterday’s messages of a service?

☐ **a)** In `/var/log/syslog` ☐ **b)** In `/var/log/messages`

☐ **c)** In the journal: `journalctl` ☐ **d)** In the unit file

5. In Windows, where do you look for failed logons?

☐ **a)** System log, Event ID 41 ☐ **b)** Security log, Event ID 4625

☐ **c)** Application log, any Error ☐ **d)** Security log, Event ID 4624