## Solutions

Each answer shows the steps, then the **result**.

**2.1**

- evidence that an adversary **has** compromised a device or network; found by analysing logs, configuration settings or files, and used to reconstruct what happened

**2.2**

(a)

- file-based

(b)

- behaviour-based

(c)

- host-based

(d)

- behaviour-based

(e)

- host-based

**2.3**

- any two of: system processes and settings, login attempts, file download attempts, user actions

**2.4**

(a)

- online password guessing

(b)

- password spraying

(c)

- credential stuffing

**2.5**

- the attack takes place on the **adversary's own computer**, using a copy of the password data they already hold; nothing is attempted against your system, so no authentication log entry is generated and there is nothing to detect

**2.6**

(a)

- the user's credentials have probably been compromised

(b)

- the evidence is about the **behaviour** of an account - where and when it logged in - found in the authentication log, rather than about the state of the host, such as a new file, process or configuration change

**2.7**

(a)

- any two of: **performance** - detection tools consume memory and processing power, and these laptops are ageing; **cost** - 300 licences is a large recurring expense; **criticality** - student laptops hold little sensitive data and provide no critical service

(b)

- **signature-based** - it is faster and uses fewer resources, so it will not slow ageing machines, and it costs less across 300 devices; the low criticality means the higher false-negative rate is an acceptable trade

**2.8**

- signature-based detection matches known patterns, so it produces almost no false positives and analysts trust its alerts; but an adversary only needs something the signature set has not seen to pass straight through, so it is easier to bypass than anomaly-based detection

**3.1 B**

- An IoC is evidence of a compromise that has already happened

**3.2 B**

- One attempt per account rules out guessing; non-default passwords rule out stuffing

**3.3 C**

- A is behaviour-based, B and D are host-based and behaviour-based respectively

**3.4 C**

- Criticality is the criterion that justifies accepting cost and performance impact

**3.5**

(a)

- **password spraying** - many different users each attempted once, within seconds, from a single IP address

(b)

- Wednesday's out-of-hours foreign login: **behaviour-based**. The privilege-elevation attempt: **behaviour-based**. Thursday's uncreated scheduled task: **host-based**. The trojan file matched by hash: **file-based**. Reason, for any one: e.g. the scheduled task is host-based because the evidence is an unauthorised change to the device's own configuration, not an account's behaviour

(c)

- Monday's spraying is **reconnaissance/initial access** attempted and failed; Wednesday's successful foreign login is **initial access** achieved with valid credentials; the privilege-elevation attempt is **lateral movement**; Thursday's scheduled task and RAT file are **persistence**, keeping access without needing to log in again

(d)

- the spraying failed, so the password was not guessed on this system; it was most likely obtained elsewhere - phished from the user, captured by a keylogger, or cracked **offline** from a stolen password file, or reused from another site's breach. None of those touch this server's authentication process, so no failed-attempt entries appear and the first sign here is a **successful** login

(e)

- Adequate on Thursday: the trojan was a known one, so its file **hash matched a signature** and signature-based detection catches it quickly and with almost no false positives. Not adequate earlier: a successful login with a valid password is not a signature of anything - it is only abnormal relative to the user's normal location and hours, which needs anomaly- or behaviour-based analysis; and detecting only at Thursday's persistence phase means the adversary already had two days inside, whereas detection at Wednesday's access phase would have limited the damage