Solutions

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

2.1

(a)

- server

(b)

- embedded computer; accept IoT only if the machine is described as networked

(c)

- handheld / mobile computer

(d)

- IoT device

2.2

(a)

- ransomware

(b)

- worm

(c)

- keylogger; accept spyware with justification

(d)

- logic bomb

(e)

- rootkit

2.3

- it is not a file - it lives in RAM, and it works through legitimate programs already installed on the device, so scanning the disk finds no malicious file and the activity looks like normal software running

2.4

- a virus must be activated by the user opening or executing a file; a worm spreads from computer to computer with no human interaction

2.5

(a)

- malware placed on an external drive runs automatically when the drive is inserted

(b)

- the machine can be booted into a special mode, bypassing the operating system and its access controls

(c)

- an exploit already exists for the known flaw, so the adversary needs no new work and little skill

(d)

- the adversary connects to the device directly through that port

2.6

- a firewall filters the data arriving at the device; without one, or with it misconfigured, malicious data reaches the device and can disrupt it or be used to take control

2.7

(a)

- **high** - patient records are sensitive data governed by law, and a publicly documented unpatched flaw makes exploitation highly likely

(b)

- **moderate** - it is weak authentication, but a printer holds little sensitive data, so the impact of compromise is limited. Accept low with a justification that impact is minimal

(c)

- **low** - the vulnerability is real, but the device is disconnected and holds only sample data, so exploiting it would have little impact

3.1 B

- A virus needs the user to open or execute a file; a trojan needs the user to install it; a logic bomb waits for a condition

3.2 B

- IoT is the everyday-device case of an embedded computer, not a general term for anything networked

3.3 B

- Living in RAM and abusing an already-installed legitimate program is exactly fileless malware. A rootkit is still a file and sits in the OS

3.4 B

- A is low, D is high, and C is not one of the criteria

3.5

(a)

- **ransomware** - the files are encrypted and a payment demand is displayed, which is its defining behaviour

(b)

- any two, each named and explained: **no anti-malware software** on the file server, so nothing stopped the malware installing; **default passwords** on the IoT sensors, which is weak authentication and gives an adversary an entry point onto the network; **unpatched scanners**, since software never updated since purchase carries known flaws with existing exploits

(c)

- **High**. The sensors are numerous and all share a known default password, so the likelihood of compromise is very high and needs no skill; and although a temperature sensor holds no sensitive data itself, it sits on the same network as the payment records, and compromising refrigeration is a **critical operation** for a firm carrying chilled freight

(d)

- The argument is **wrong**. Risk is not only about the data the device holds - an unpatched device on the network is a route to the devices that do hold sensitive data, which is exactly the lateral-movement path an adversary needs. Twenty devices never updated since purchase carry every flaw published since then, so likelihood is high even if the direct impact is low; and losing scanning would halt warehouse operations, so the impact is not negligible either

(e)

- Three controls each matched to a different vulnerability - install and maintain anti-malware on the file server; change every default password and enforce a password policy on the sensors; establish a patching schedule for the scanners. First: **change the default passwords**, because it costs almost nothing, removes the highest-likelihood route in, and closes forty devices at once. Accept "restore from backup and patch the server first" if justified by the live incident