## Solutions

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

**2.1**

- ARP is used by the default gateway to build a table pairing IP addresses with MAC addresses, so traffic addressed to an IP reaches the correct physical device

**2.2**

- ARP has no authentication, so a false pairing of the adversary's MAC with a legitimate IP is accepted; traffic intended for that device is then delivered to the adversary, who can read, alter or drop it

**2.3**

- the adversary sends the switch many Ethernet frames, each carrying a different MAC address; this overwhelms the switch's address table, forcing it into broadcast mode so every frame goes to every port - including the adversary's

**2.4**

(a)

- DNS poisoning

(b)

- smurf attack

(c)

- MAC flooding

**2.5**

- ARP poisoning - interception; DNS poisoning - redirection; smurf - denial of service

**2.6**

(a)

- an adversary plugs directly into the port and, without port security, the switch accepts the device onto the LAN, giving them a position inside the network from which to launch further attacks

(b)

- the signal broadcasts beyond the physically secure space, so the adversary can pick up signals and beacon frames from outside the building and attempt to join or to break the encryption without ever entering

(c)

- an adversary can plug a wireless access point into it, creating a **rogue access point**, which gives them - and anyone else in range - wireless access to the internal network

**2.7**

- any three of: flood the network to create a denial of service; map the internal structure of the network; spoof a legitimate device

**2.8**

- it checks networks, devices and applications for **known** vulnerabilities and produces a report, usually with a severity rating for each finding. Limitation, any one: it finds only vulnerabilities already known and catalogued, so a novel flaw is missed; it reports the vulnerability but not whether an adversary is capable of exploiting it; and a report is not a fix

**2.9**

(a)

- **moderate to high** - the impact is high because payroll data would be captured, but exploitation requires advanced technical ability and sustained effort, which reduces the likelihood; accept either rating if the answer weighs impact against difficulty

(b)

- **moderate** - it gives an adversary information about the systems or devices on the network without granting access

(c)

- **low** - it would be difficult to exploit given the physical control, and the likely negative impact is minimal

**3.1 B**

- Domain names to IP addresses is DNS; MAC to switch port is the switch's own table

**3.2 B**

- It floods the network with ICMP requests so it cannot serve legitimate users

**3.3 B**

**3.4 B**

- That is the definition of the moderate rating

**3.5**

(a)

- any three of: plug into the reception data port, which has no port security; join the Wi-Fi, which does not authenticate devices; break the weak wireless encryption from the car park; plug a rogue access point into the open store-room port. Easiest: **joining the Wi-Fi**, because it authenticates neither devices nor users and needs no physical entry at all. Maximum 4

(b)

- an adversary can plug a wireless access point into the open port, creating a **rogue access point** that gives them continuing wireless access to the internal network from outside the building, without needing to return to the store room

(c)

- any two, each named with its harm: **ARP poisoning** - false IP-to-MAC pairings so membership traffic including bank details is delivered to the adversary, who can read or alter it; **MAC flooding** - overwhelming the switch so it broadcasts, exposing till and membership traffic; **DNS poisoning** - redirecting staff to a fake login page; **smurf** - flooding with ICMP so the till system is unavailable and the centre cannot trade. Maximum 4

(d)

- It is **wrong**. A scanner checks for **known** vulnerabilities only, so a novel technique or a flaw not yet catalogued does not appear, and no report is complete. A report is also only a list: it does not fix anything, and it says nothing about the network's design faults here - a single flat network with no segmentation is a serious weakness that no individual scan finding would name

(e)

- **High**. An adversary can join with essentially no skill and no physical access, and once inside can capture traffic and spoof devices - the "easily, with significant impact" definition - against data that includes bank details. First two changes, any two justified: enable **device and user authentication** on the Wi-Fi and strengthen its encryption, which closes the easiest route; enable **port security** on the reception port and disable the unused store-room port, which closes the physical routes. Accept network **segmentation** separating the till and membership systems from guest traffic as one of the two, with justification