MODULE G SECURITY · G9

Preventing attacks 3: mark scheme

21 marks · OCR J277 spec 1.4.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative answers; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. **NE** = not enough. **BOD** = benefit of the doubt. Spec points covered (J277 1.4.2): common prevention methods (penetration testing, encryption, physical security; firewalls only as a contrast in Q1 and Q5); what each prevention method may limit/prevent and how it limits the attack; methods to remove vulnerabilities; how to limit the threats posed in 1.4.1. Anti-malware, user access levels and passwords (also 1.4.2) are tested in G7/G8. This part is OCR only: Cambridge 0478 5.3.2 does not list penetration testing or physical security.

QUESTION	ANSWER	MARKS	GUIDANCE
1 J277 1.4.2	Keycard to open the server room door: physical security Security team tries to break in, with permission: penetration testing Data scrambled using a key: encryption Incoming traffic checked against rules: firewall	**4**	1 mark per correct row. Anti-malware is not used. Accept "pen testing" / "penetration test". Ignore spelling if the method is clear.
2(a) J277 1.4.2, 1.4.1	Lock the server room door // fit a keycard / keypad / biometric lock (1) ... so only authorised staff can get in // the visitor cannot reach the servers (1) Security guard / reception desk that signs visitors in // visitors must be escorted (1) ... so visitors cannot walk into the server room on their own (1) Keep the servers in a locked cabinet / rack // physically lock / block the USB ports (1) ... so nothing can be plugged in even if someone enters the room (1) CCTV / alarm on the server room (1) ... deters the visitor // the person can be identified // staff are alerted quickly (1)	**2**	Mark in pairs: 1 for a physical security method, 1 for how it limits this threat. The second mark depends on the first. Do not award software methods (e.g. anti-malware, firewall, encryption, passwords): they are not physical security. "Security" / "protect the room" alone = NE. Credit any other valid physical security method with a matching explanation.
2(b) J277 1.4.2, 1.4.1	Lock the laptop in a drawer / cabinet / safe overnight (1) ... so it cannot be picked up from the desk (1) Cable lock fixing the laptop to the desk (1) ... so it cannot easily be carried away (1) Lock the office // keycard / biometric entry to the office (1) ... so only authorised people can get to the desk after hours (1) Alarm / security guard / night patrol (1) ... stops or interrupts a break-in // staff / guards are alerted (1) CCTV (1) ... deters theft // the thief can be identified (and the laptop recovered) (1)	**2**	Mark in pairs as 2(a). Do not award encryption or a password here: they protect the data, not the laptop, and are not physical security. The same method as 2(a) can score again if the explanation is applied to the laptop. Credit any other valid physical security method with a matching explanation.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.2	Penetration testing simulates a real attack (on the new page) // an authorised person tries to break in It finds vulnerabilities / weaknesses (e.g. in the login, search box, payment form or database) ... before real attackers / criminals can find and exploit them The weaknesses are reported so they can be fixed / removed before the page goes live Reduces the risk of customer (login / payment) details being stolen // of attackers getting in through the new page	**3**	1 mark per bullet, max 3. "To check it is secure" / "to test it" alone = NE. Do not award answers saying penetration testing *stops* attacks by itself: it finds weaknesses, and fixing them limits attacks. Credit any other valid point.
3(b) J277 1.4.2, 1.4.1	Brute-force attack (e.g. on customer logins) SQL injection (e.g. through the login or search box) Denial of service (DoS / DDoS) Social engineering / phishing (e.g. of staff) Malware Data interception	**2**	1 mark each, max 2. Mark the first answer on each line. Two answers that are the same attack (e.g. "DoS" and "DDoS") = 1 mark. "Hacking" alone = NE. Credit any other valid form of attack from J277 1.4.1.
3(c) J277 1.4.2	A penetration tester has permission (from the owner) // is authorised / employed / paid by the company; a criminal attacker does not have permission A penetration tester reports the weaknesses so they can be fixed; a criminal attacker exploits them // steals / changes / deletes data A penetration tester does not damage the system or keep the data	**1**	Any one. Mark the first answer only. Only one side of the difference needs to be stated if the other is clearly implied. "One is legal" alone = BOD. "Uses different tools" = 0.
4(a) J277 1.4.2, 1.4.1	The data on the drive is scrambled / encoded (using a key / an encryption algorithm) The thief cannot understand the customer data // the data is meaningless ... without the (correct) key Only the company (with the key) can decrypt it / turn it back into the original data	**2**	1 mark per bullet, max 2. "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Do not award "the drive cannot be stolen" or "stops the data being taken": encryption does not stop theft.
4(b) J277 1.4.2, 1.4.1	Data interception (e.g. when customer data is sent over the internet / a network) // packet sniffing Theft of data by someone who gets unauthorised access to the server / database (e.g. a hacker or SQL injection), because the stolen data is meaningless A member of staff copying the files without permission Theft of another device / storage medium holding the data (e.g. the laptop in Q2(b))	**1**	Any one. Mark the first answer only. Do not accept denial of service, brute-force or phishing alone: encryption does not limit these. "Hacking" alone = NE unless linked to stealing the data. Credit any other valid answer.

QUESTION	ANSWER	MARKS	GUIDANCE
5 J277 1.4.2	**Physical security** A firewall only checks / filters network traffic (between the network and the internet) // it does nothing to stop someone physically reaching the servers Someone in the building could steal / damage a server or copy data from it (e.g. with a USB drive) without going through the firewall Physical security (e.g. locks / keycards / CCTV / guards) stops or limits unauthorised people getting to the servers **Penetration testing** The firewall may be set up wrongly / have weak rules // the system may have other vulnerabilities that a firewall does not stop Some attacks (e.g. SQL injection or brute-force on the login page) arrive in traffic the firewall allows through to the website Penetration testing finds these weaknesses (including in the firewall set-up) so they can be fixed before attackers exploit them	**4**	1 mark per bullet, max 4. Max 2 if only physical security **or** only penetration testing is addressed. "A firewall is not enough" / "hackers can get past it" alone = NE: must say why. Credit any other valid point (e.g. a firewall does not limit threats from staff already inside the building).

Total: 21 marks