MODULE G SECURITY · G3

Brute-force attacks: mark scheme

20 marks · OCR J277 spec 1.4.1 (brute-force attacks: how the attack is used, its purpose) and 1.4.2 (passwords: how they limit the attack)

How to use. One mark per bullet up to the maximum shown. **/** separates alternatives; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. NE = not enough. For "give / state two" items, mark the first two answers only. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	Trial and error: True Tricking a person: False Automated, many passwords quickly: True Purpose is unauthorised access: True One more character reduces combinations: False	**5**	One mark per correct row. A row with both boxes ticked scores 0. Row 2 describes social engineering, not brute force.
2(a) J277 1.4.1	(The attacker uses) software / an automated program (to make the guesses) It tries (a member's username with) password after password // trial and error ... (systematically) trying every possible combination (of characters) Common / weak passwords / dictionary words may be tried first Huge numbers of attempts are made very quickly / per second Until the correct password is found / one works, (then the attacker logs in)	**3**	Max 3. Do not accept "hacks the account" or "guesses the password" alone (NE): the answer must show repeated / systematic attempts. Do not credit tricking the member or phishing (social engineering).
2(b) J277 1.4.1	Steal / view the member's personal data (name / address) Steal / use the payment card details // make payments / hire bikes with the member's card Change / delete the member's data // change the password to lock the member out Sell the data (to others) Use the details for identity theft / fraud Install / spread malware // use the account to attack the company's system	**2**	1 mark each, max 2. Do not accept "get into the account" / "gain access" (repeats the question). Two answers that are the same idea (e.g. "steal data" and "take data") = 1 mark.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.1, 1.4.2	Each extra character multiplies / greatly increases the number of possible passwords / combinations // e.g. 4 letters = 456,976 but 8 letters = about 209 billion So it takes (much) longer to try them all // e.g. under 0.1 seconds for 4 letters but about 6 hours for 8 letters ... so the attacker may give up / be detected (before the password is found)	**2**	Max 2. Credit figures quoted from the table as the evidence. Do not accept "more secure" / "harder to guess" alone (NE).
3(b) J277 1.4.1, 1.4.2	More possible characters for each position (62 instead of 26) So there are (many) more possible combinations (for the same length) // e.g. about 218 million million (218,340,105,584,896) instead of about 209 billion So it takes much longer to try every combination // e.g. about 253 days instead of about 6 hours	**2**	Max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone (NE).
4(a) J277 1.4.2	C	**1**	Correct answer only. Accept the password written out instead of the letter.
4(b) J277 1.4.2	It is long / has 12 characters // it is the longest option It mixes uppercase and lowercase letters It contains digits / numbers It contains symbols / special characters It is random / is not a (dictionary) word / name // has no pattern or repeated characters	**2**	1 mark each, max 2. If 4(a) is not C, award marks only for features that are true of the password the student chose and that do make it harder to find (e.g. B: uppercase letter, digits). Do not accept "it is complicated / strong" alone (NE).
5(a) J277 1.4.1, 1.4.2	A brute-force attack needs to make a (very) large number of attempts / guesses Only five guesses can be made before the account is locked ... so the attack is slowed down (to a few guesses every 30 minutes) // the number of guesses that can be made is greatly reduced So it would take far too long to try every / enough combinations // the password is very unlikely to be found Repeated lock-outs can alert the user / the firm (that an attack is happening)	**3**	Max 3. Do not accept "stops hackers" or "makes it more secure" alone (NE). Allow "the attack is stopped / blocked" for the second or third point only if linked to the limited number of attempts.

Total: 20 marks