MODULE G SECURITY · G3

Brute-force attacks

Original practice questions · 20 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1, 5.3.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **20 marks**.

1

Total: 1 mark

(a) Tick (✓) **one** box to show which description is a brute-force attack. **[1]**

Description	✓
Sending a very large number of requests to a web server so it cannot respond to real users	
Using a program to try one password after another until the correct one is found	
Redirecting a user from a genuine website to a fake one without their knowledge	
Sending an email that pretends to be from a trusted organisation to get personal details	

2

Total: 6 marks

A hotel chain lets guests book rooms through an online account. Each account is protected by a username and password, and stores the guest's bookings and payment card details.

(a) Describe the process involved in a brute-force attack on a guest's account. **[3]**

(b) Tick (✓) **one** box in each row to show whether each one is a possible aim of a brute-force attack on a guest's account. **[3]**

Possible aim	Yes	No
To obtain the guest's payment card details		
To make the hotel's website unavailable by flooding it with requests		
To change or cancel the guest's bookings		

3 **Total: 4 marks**

The table shows how many different passwords are possible for some password rules. It also shows how long it would take to try every one of them, assuming the hacker's software tries 10 million passwords per second.

Characters allowed	Length	Possible passwords	Time to try them all
Lowercase letters only (26)	4	456,976	less than 0.1 seconds
Lowercase letters only (26)	6	308,915,776	about 31 seconds
Lowercase letters only (26)	8	208,827,064,576	about 6 hours
Upper and lowercase letters and digits (62)	8	218,340,105,584,896	about 253 days

(a) Explain, using the table, how the length of a password affects the chance of a brute-force attack being successful. **[2]**

(b) Explain, using the table, why the hotel should require passwords that contain a mixture of character types. **[2]**

4 **Total: 6 marks**

The hotel chain wants to reduce the risk of a brute-force attack on a guest's account being successful. Explain how each security solution helps.

(a) Locking the account after a set number of failed log-in attempts. **[2]**

(b) Two-step verification. **[2]**

(c) Letting guests log in to the hotel's app with a fingerprint (biometrics) instead of a password. **[2]**

5 **Total: 3 marks**

(a) Complete the sentences using words from the list. Not all of the words are used. **[3]**

combination · encryption · hardware · packet · phishing · software · trial and error

A brute-force attack finds a password by ....., trying every possible ..... of characters until one works. It is carried out using ....., so a huge number of attempts can be made every second.

Total for this worksheet: 20 marks