MODULE G SECURITY · G9

Preventing attacks 3: penetration testing, physical security and encryption

Original practice questions · 21 marks · ~25 minutes · OCR J277 spec 1.4.2

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 **21 marks**.

1

Total: 4 marks

Complete the table by writing the prevention method that each description matches. Choose from the list. Not all methods are used. **[4]**

anti-malware · encryption · firewall · penetration testing · physical security

Description	Prevention method
Staff must swipe a keycard to open the door of the room where the servers are kept.	
A company pays a security team to try to break into its systems, with permission, and report the weaknesses it finds.	
Data is scrambled using a key, so that anyone who intercepts it cannot understand it.	
Traffic coming in from the internet is checked against a set of rules, and traffic that breaks the rules is blocked.	

2 **Total: 4 marks**

A company sells concert tickets through its website. Its servers are kept in a room on the ground floor of a shared office building. People from other businesses use the same main entrance.

Describe how physical security could limit each of these threats.

(a) A visitor walks into the unlocked server room and plugs a USB drive into one of the servers. **[2]**

(b) A laptop that holds customer records is left on a desk in the office and is taken overnight. **[2]**

3 **Total: 6 marks**

The ticket company is about to launch a new web page where customers log in, search for concerts and pay for tickets.

(a) Explain why the company should have penetration testing carried out before the new page goes live. **[3]**

(b) Give **two** types of attack that a penetration tester could simulate on the new page. **[2]**

1

2

(c) State **one** difference between a penetration tester and a criminal attacker. **[1]**

4 **Total: 3 marks**

Every Friday, a backup copy of the customer database is saved onto an external hard drive. A manager carries the drive to the company's second office. The backup is encrypted.

(a) Explain how encrypting the backup limits the threat if the drive is stolen on the way. **[2]**

(b) State **one** other threat to the customer data that encryption could help to limit. **[1]**

5 **Total: 4 marks**

The company's IT manager says: "Our firewall keeps attackers out, so we don't need physical security for the servers and we don't need penetration testing."

Explain why the IT manager is wrong. Refer to **both** physical security **and** penetration testing in your answer. **[4]**

Total for this worksheet: 21 marks