MODULE G SECURITY · G4

Distributed denial of service (DDoS) attacks

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

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: 5 marks

(a) Tick (✓) **one** box to show the aim of a distributed denial of service (DDoS) attack. **[1]**

Aim	Tick (✓)
To find a password by trying every possible combination	
To intercept data while it is being sent across a network	
To stop genuine users from accessing a website or server	
To send a user to a fake website when they type in a real web address	

(b) The word *distributed* in distributed denial of service tells you where the attack comes from. State what it tells you. **[1]**

(c) Tick (✓) **one** box in each row to show whether each statement about DDoS attacks is true or false. **[3]**

Statement	True	False
A DDoS attack sends a very large number of requests to a server at the same time.		
The owners of the computers used in a DDoS attack usually know that their computers are being used.		
The usual aim of a DDoS attack is to copy the data stored on the server.		

2 **Total: 4 marks**

(a) The statements **A** to **F** describe the process of a DDoS attack on a web server. Statement **A** is the first step. Write the numbers **2** to **6** in the table to show the order of the other steps. **[4]**

	Statement	Order
A	The attacker spreads malware to many computers, for example in infected email attachments.	**1**
B	The web server cannot respond to all of the requests.	
C	The attacker sends an instruction to the bots to start the attack on a chosen web server.	
D	Genuine users cannot access the website because the web server is very slow or has crashed.	
E	Each infected computer becomes a bot, and together the bots form a botnet that the attacker controls.	
F	The bots all send large numbers of requests to the web server at the same time.	

3 **Total: 6 marks**

A bus company has a journey-planner website that customers use to find bus times and buy tickets. The website is stored on the company's web server. One morning the web server suffers a DDoS attack.

(a) Explain why customers cannot use the journey planner during the attack. **[3]**

(b) During the attack, the company receives a message from the attackers. The message demands money to stop the attack. Identify the aim of this attack. **[1]**

(c) Give **two other** aims a person might have for carrying out a DDoS attack on a company. **[2]**

1

2

4 **Total: 2 marks**

A technician at the bus company finds the IP address of one of the computers sending requests to the web server. The technician blocks this IP address, but the attack continues.

(a) Explain why blocking this IP address does not stop the attack. **[2]**

5 **Total: 3 marks**

A manager at a different company says: "Every computer in our office has up-to-date anti-malware software, so our web server cannot suffer a DDoS attack."

(a) Explain why the manager is **not** correct. **[3]**

Total for this worksheet: 20 marks