MODULE G SECURITY · G4

DDoS attacks: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (describe the processes involved in, and the aim of carrying out, a range of cyber security threats, including a distributed denial of service (DDoS) attack)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	To stop genuine users from accessing a website or server	**1**	More than one tick = 0.
1(b) 0478 5.3.1	The attack / requests come from many computers / devices (at the same time) // from many different places / sources // from a botnet	**1**	Do not accept "it is spread out" / "it is shared" alone. Do not accept "it attacks many servers".
1(c) 0478 5.3.1	Very large number of requests at the same time: True Owners usually know their computers are used: False Usual aim is to copy the data on the server: False	**3**	One mark per correct row. A row with both boxes ticked scores 0.
2(a) 0478 5.3.1	Correct order: A 1, **E 2**, **C 3**, **F 4**, **B 5**, **D 6** One mark for each of E, C, F, B, D with the correct number (max 4)	**4**	max 4: all five correct = 4. A number used twice: mark neither statement with that number.
3(a) 0478 5.3.1	Any three from: Many computers / bots (in a botnet) send requests to the web server A (very) large number of requests is sent at the same time The web server cannot handle / respond to all the requests // is overloaded / flooded The web server slows down / fails / crashes / times out The customers' (genuine) requests cannot reach the web server // are not answered	**3**	max 3. Do not credit "the customers' computers are infected" / "the data is stolen" / "the website is hacked" alone.
3(b) 0478 5.3.1	To get money from the company // to demand a ransom // extortion / blackmail	**1**	Do not accept "to steal money" / "to steal data".

QUESTION	ANSWER	MARKS	GUIDANCE
3(c) 0478 5.3.1	Any two from: To disrupt the company // stop its service being used To make the company lose money / sales To damage the company's reputation Revenge // a grudge against the company As a protest // to make a political point For entertainment // for fun // to show they can As a distraction while another attack takes place To help a competitor To test how well a system copes with heavy traffic // to test its resilience	**2**	max 2. Credit any other valid aim. Do not credit demanding money / ransom again (it is the aim in (b)). Do not accept "to steal data" alone.
4(a) 0478 5.3.1	Any two from: The requests come from many (different) computers / bots Each computer / bot has a different IP address // there are many IP addresses The other bots keep sending requests // blocking one removes only a very small part of the traffic The web server is still overloaded (by the requests from the other bots) The attack traffic is hard to tell apart from genuine users' requests	**2**	max 2. Do not accept "the attacker is too clever" / "the attack is too strong" alone.
5(a) 0478 5.3.1	Any three from: The bots are (usually) other people's computers, not the company's own computers The bots / botnet can be anywhere (in the world) // outside the company The attack works by sending (large numbers of) requests to the web server (over the internet) The web server does not need to be infected with malware for the attack to work Anti-malware on the office computers cannot stop the requests being sent // reaching the web server Any web server that is connected to the internet can be a target	**3**	max 3. Do not credit "anti-malware does not work" / "anti-malware can be out of date" (the stem says it is up to date) without a point about how the attack works.

Total: 20 marks