MODULE G SECURITY · G4

Denial of service attacks: mark scheme

20 marks · OCR J277 spec 1.4.1: forms of attack, denial of service attacks (threats posed to devices/systems, how the attack is used, the purpose of the attack)

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. Credit any other valid answer that shows the same understanding. A distributed denial of service (DDoS) attack is a form of denial of service attack: accept DDoS descriptions anywhere, but never require the term DDoS or botnet.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	Stops genuine users accessing a website / network: True Floods a server with more requests than it can handle: True Attacker must know a user's password: False Main aim is usually to copy the data on the server: False	**4**	1 mark per correct row. 2+ ticks in a row = 0 for that row.
2(a) J277 1.4.1	(The attacker) sends / floods the (web) server with a very large number of requests / traffic ... more requests than the server can handle / process // uses up the server's resources / the bandwidth available The server slows down / cannot respond / crashes Genuine customers' requests are not answered // customers cannot access / load the booking website The requests may be sent from many devices at the same time	**3**	1 mark per bullet, max 3. Must be an attack on the **server / website / network**. Do not credit answers that describe an attack on a customer's own computer. Do not accept "hacks the website" / "puts a virus on the server" / "steals the data". A description of how to prevent the attack scores 0.
2(b) J277 1.4.1	Cannot load / access the booking website // the website times out The website is very slow (to respond) Cannot book / buy tickets (online) at that time Cannot check / change / cancel an existing booking May have to book another way (e.g. by phone) // may book with a different company May miss out on a sailing / ticket offer	**2**	1 mark per bullet, max 2. Mark the first two answers. Two answers that say the same thing (e.g. "cannot access the site" and "cannot load the page") = 1 mark. Do not accept "their data is stolen" / "their computer gets a virus".

QUESTION	ANSWER	MARKS	GUIDANCE
2(c) J277 1.4.1	Customers cannot book (1) ... so tickets are not sold / income is lost while the website is down (1) Customers may book with a competitor instead // may not come back (1) Damage to the company's reputation // customers lose trust in the company (1) ... so fewer bookings in future (1) Cost of staff time / experts to get the website working again (1) Cost of paying for extra protection / a bigger server / more bandwidth (1) Cost of refunds / compensation to customers who missed out (1)	**2**	1 mark per point, max 2. Two separate points, or one point and its expansion. Do not accept "they lose money" alone (repeats the question). Do not credit a ransom being paid unless linked to the attackers demanding payment.
3(a) J277 1.4.1	To disrupt the organisation // stop it providing its service To make the organisation lose money / income To damage the organisation's reputation To demand money to stop the attack // extortion / blackmail As a protest // to make a political point Revenge // a grudge (e.g. a former employee) As a distraction while another attack takes place To help a competitor // to stop customers using a rival For fun // to show they can do it	**2**	1 mark per bullet, max 2. Credit any other valid reason. Do not accept "to steal data" alone (a denial of service attack does not usually steal data); accept "to distract the organisation while data is stolen". Do not accept "ransom" alone without reference to payment to stop the attack.
4(a) J277 1.4.1	The devices have been infected with malware (e.g. from an email attachment / download) The malware lets the attacker control the devices (remotely) // the devices become bots / zombies / part of a botnet The attacker instructs the devices to send requests to the (ferry company's) server (at the same time) The malware runs hidden / in the background, so the owners do not notice	**2**	1 mark per bullet, max 2. Do not require the words bot / botnet. Accept "virus / Trojan" for malware. Do not accept "they have been hacked" alone.
4(b) J277 1.4.1	The requests come from many different devices // many different IP addresses / locations ... so blocking one device / IP address does not stop the others It is hard to tell the attack traffic from genuine customers' traffic // blocking the traffic could also block real customers Many devices together send far more requests than one computer could	**2**	1 mark per bullet, max 2. Do not accept "it is more powerful / bigger" alone. Do not accept "the devices are in other countries" alone (repeats the stem) unless linked to blocking.

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) J277 1.4.1	A denial of service attack aims to make the website / service unavailable, not to steal data It works by flooding the server with requests // it does not need to break into / log in to the server ... so customers' data is not usually accessed / stolen by this attack The slow website was caused by too much traffic / the server being overloaded, not by a break-in However, the attack could have been a distraction for a different attack, so the company should still check // data could only be stolen by a separate attack	**3**	1 mark per bullet, max 3. Full marks are possible without the final ("however") point. Do not credit answers that agree with the manager. Do not accept "the data is encrypted" / "they have a firewall" (not what the attack does).

Total: 20 marks