1.3 EXCHANGING DATA · 1.3.3

Network security & threats — Mark scheme

33 marks · spec 1.3.3(c)

AO key: AO1 = knowledge & understanding · AO2 = application · AO3 = reasoned judgements. Accept any valid alternative; do not award the same point twice.

Q	ANSWER	AO	MARKS
1(a)	Malicious software designed to damage / gain unauthorised access to a system. (1)	AO1	1
1(b)	A virus attaches to a host file and spreads when that file is run (1); a worm spreads by itself across a network without a host file (1). (2)	AO1	2
1(c)	It encrypts/locks the user's files (1) and demands payment to restore access (1). (2)	AO1	2
1(d)	Any one: scans for and removes known malware · runs in the background to detect new infections · quarantines suspicious files. (1)	AO1	1

Q	ANSWER	AO	MARKS
2(a)	Phishing. (1)	AO1	1
2(b)	It targets the user, not the technology (1); a person can be deceived into giving away their credentials even when the network defences are strong (1). (2)	AO2	2
2(c)	Any one developed: staff training to spot phishing (1) so they don't click suspicious links (1); OR two-factor authentication (1) so a stolen password alone is not enough (1). (2)	AO2	2

Q	ANSWER	AO	MARKS
3(a)	The attacker enters SQL code into an input field (e.g. the username box) (1); because the input is not validated it becomes part of the query (1); e.g. a condition that is always true returns data / grants access (1). (3)	AO2	3
3(b)	Max 3, e.g.: • validate / sanitise user input (1) • use parameterised queries / prepared statements (1) • so input is treated as data, not executable code (1)	AO2	3

Q	ANSWER	AO	MARKS
4(a)	A server is flooded with a huge number of requests (1) so it cannot respond to legitimate users / goes offline (1). (2)	AO1	2
4(b)	It inspects traffic against a set of rules (1) and blocks anything not allowed (e.g. suspicious ports/addresses) (1). (2)	AO1	2

Q	LEVELS-OF-RESPONSE MARK SCHEME	AO	MARKS
5	Mark using the levels descriptors below. AO1 (knowledge of threats/measures), AO2 (application to the hotel), AO3 (justified recommendations). **LEVEL** / **DESCRIPTOR** **Level 3 (9–12)**: Identifies a range of relevant threats and matched protective measures, clearly **applied** to the hotel's data, with **justified** recommendations. Well structured. **Level 2 (5–8)**: Covers several threats and measures with **some** application and partial justification. **Level 1 (1–4)**: Basic list of threats or measures with little application to the hotel or justification. **0**: Nothing creditworthy. **Indicative content** (credit any valid point): • Threats: malware stealing/corrupting the customer database; phishing tricking staff into revealing logins; DoS taking the booking site offline; SQL injection exposing accounts via the login/search box. • Encryption of stored card details and data in transit (HTTPS) so intercepted/stolen data is unreadable. • Firewall to filter traffic; anti-malware and prompt patching to reduce infection. • Input validation to stop SQL injection; strong authentication / access rights for staff. • Staff training against phishing; regular backups to recover from ransomware. • Justified, layered recommendation prioritising the card data (encryption + access control).	AO1 ×4 AO2 ×4 AO3 ×4	**12**

Total for paper: 33 marks