Making IT good for society

BCS Level 4 Certificate in Security Technology Building Blocks
Answer Key and Rationale – QAN 603/0884/9

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	During mutual authentication, both remote systems authenticate each other at the same time.	1.1
2	**C**	This statement captures the input and checks if it's a number. This check on its own would not prevent the rest of the answers from occurring.	3.1
3	**D**	D is an undesirable feature because a firewall also has to allow network traffic to flow back into your network from the Internet. The other responses are good features of a firewall.	2.1
4	**A**	Passwords should be frequently changed between 3 to 6 months.	1.4
5	**C**	Policy-based routing provides a tool for forwarding and routing data packets based on policies defined by network administrators. It is a way to have the policy override the routing protocol decisions.	2.2
6	**B**	The correct answers are: Proxies - as proxies have this facility built in. Firewall - as firewall rules can limit traffic based on country of origin. NIDS - (like Snort) can also inspect traffic for IP address and similar for country of origin.	3.3
7	**C**	A service level agreement (SLA) forms part of the contract between a business and its IT supplier.	2.2
8	**B**	One common use of a hash function is to check whether a file or data string has been altered. If the same file is hashed at two different times and the hashes differ, the file has been changed.	1.2
9	**A**	Only CREST provides accreditation for the organisations. The others are the certification bodies for professionals.	4.3
10	**C**	The purpose of a RADIUS server is to provide AAA (centralised Triple A management) for users logging in to a network.	2.1
11	**C**	A zero-day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware.	1.3
12	**A**	Scanning is done in the second step of penetration testing (the first phase is reconnaissance). These two steps constitute the pre-attack phase.	2.1

Question	Answer	Explanation / Rationale	Syllabus Sections
13	**D**	A service level agreement (SLA) is a contract between a service provider (contractor in this question) and the end user (enterprise in this question) that defines the level of service expected from the service provider.	2.2
14	**A**	A DMZ is a physical or logical subnetwork that contains and exposes an organisation's external-facing services to an untrusted network, usually the Internet.	2.2
15	**B**	HTTPS use port 443 by default.	2.3
16	**A**	Biometrics are generally considered as the most reliable identification technologies compared to the others. This does not imply that they don't have any shortcomings. But among the different factors of authentication, 'what you are' is more reliable than 'what you know' and 'what you have'.	3.2
17	**D**	The purpose of a parameterised query is to allow the data source to be able to distinguish executable statements from untrusted data; and hence it protects database from SQL injection attacks.	3.4
18	**A**	SANS Top 20 Critical Security Controls are a set of IT-based controls and therefore physical protection is not covered in this category.	4.1
19	**D**	The purpose of a DMZ is to add an additional layer of security to an organisation's local area network (LAN) The DMZ functions as an isolated network positioned between the Internet and the private network.	4.2
20	**A**	It captures data and a transducer is then used to automatically convert the actual image or a sound into a digital file.	4.4