BCS Level 4 Certificate in Network Security
Answer Key and Rationale – QAN 603/0546/0

Question	Answer	Explanation / Rationale	Syllabus Sections
1	A	A quarantine network would contain devices to allow updates and patches to be installed on the non-compliant device.	2.3
2	D	A honeypot is designed to attract potential attackers to deflect them from the real network.	2.1
3	A	A stateful packet inspection firewall checks outbound communication and will only allow inbound if it's part of an ongoing legitimate communication. Intrusion prevention drops packets when identifying suspicions traffic. Intrusion detection only alerts when suspicious traffic is identified. Application layer protocol analyses all ISO layers to identify suspicious traffic.	2.4
4	C	Accountability determines what the user did when on the network.	2.1
5	C	All viruses are malware but not all malware are viruses. Some forms of adware are malware; however, some can be legitimate advertising.	2.3
6	D	An email worm distributes copies of itself in an infectious email attachment.	1.1
7	D	BS 25999 defines MTPOD as 'the duration after which an organisation's viability will be irrevocably threatened if product and service delivery cannot be resumed'.	1.2
8	B	Denial of service attempts to overload a system by flooding it with unnecessary requests from false source IP addresses.	1.1
9	C	DHCP is the standard method for automatically providing IP configuration to a client host.	1.2
10	C	DNS poisoning causes the DNS server to return an incorrect IP address.	1.1
11	A	Driver signature enforcement prevents users installing drivers not signed by Microsoft.	2.3
12	B	EFS is the embedded system which Windows uses to encrypt files.	2.2
13	B	FTP is assigned the port numbers 20 and 21	2.4
14	C	Intrusion prevention system (IPS) detects and removes suspicious packets.	2.4
15	B	Kerberos is used to authenticate and encrypt communications. The others are not inherently secure.	1.2
16	A	Microsoft have published the group policy processing order as: local, site, domain, OU.	2.2
17	C	Modems use telephone numbers. War dialling uses telephone numbers to initiate the attack.	1.2

Question	Answer	Explanation / Rationale	Syllabus Sections
18	B	NAT translates a router's public IP address to a LAN private address or vice versa.	2.1
19	A	Network based IDS will cover the whole network. Host based IDS will cover individual devices only.	2.4
20	C	NTFS is the correct answer because it is the only file system that allows configuration of permissions on files and folders. Both FAT32 and FAT16 can be used on Windows systems. XFS is a Linux file system.	2.2