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
21	B	OS hardening means that you remove anything unnecessary from the system to provide a smaller attack surface.	2.1
22	C	Packet filtering works on the basis of IP address or port number.	2.4
23	D	Protection should be installed before leaving the machine vulnerable.	2.3
24	C	RSA is the only asymmetric algorithm in the list. The rest are symmetric algorithms.	2.2
25	A	Secure Shell (SSH) is the common protocol used for this purpose. FTPS and SCP are file transfer protocols, HTTP is not secured.	1.2
26	D	Social engineering is dependent on people's awareness and isn't a technology issue.	1.1
27	C	Social engineering relies on human interaction and often involves tricking people into breaking normal security procedures. War dialling automatically scans lists of telephone numbers. Brute force attempts to discover passwords. Man-in-the-middle attacks are where an attacker intercepts messages from a sender and / or receiver and can alter the message.	1.1
28	D	Stateful firewalls track network connections.	2.4
29	D	SYN flooding takes place when thousands of packets are sent to a device. The result is a denial of service attack.	1.2
30	C	Tailgating is a form of social engineering attack.	2.1
31	B	TFTP is used for transferring files and is used where user authentication is not required; it uses UDP. FTP and SFTP use TCP. RPC is a remote procedure call.	1.2
32	C	The account settings group policy sets a minimum length of seven characters for a password in Windows Server 2012.	2.2
33	C	The first thing is to remove the device from the network. Remedial action for the network can take place after that.	2.3
34	C	The group policy for the Finance group means that only users in that group will be affected. Any of the other options may affect other users unintentionally.	2.2
35	A	The principle of least privilege states that users need only the minimum permissions to do their job.	2.1
36	A	Trojan horse is a program that suggests it is one thing but contains malicious code.	1.1
37	A	UPS is a universal power supply that runs off battery when the electricity supply fails.	2.1

Question	Answer	Explanation / Rationale	Syllabus Sections
38	C	User account control is designed to prevent non-administrative users changing settings. Malware would have to have admin privileges to change the system. AppLocker restricts the software a user can use on a system. BitLocker encrypts a system.	2.3
39	D	Whaling targets high profile targets in a company because of the information they have, or the access to the network they have.	1.1
40	A	When accessing a folder remotely, both NTFS and shared permissions are used to secure the access.	2.2