BCS Level 4 Certificate in Network Security
QAN 603/0546/0

Specimen Paper A

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 20 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

Pass mark is 13/20.

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.

This qualification is regulated by Ofqual (in England).

1 A company has a policy that only allows compliant devices to join their network. What would be put in place to ensure that devices could become compliant?

A Quarantine network.
B Demilitarised zone.
C Virtual private network.
D Virtual local area network.

2 A network engineer may set up a sacrificial server on a network to gather information about intruders. What is this called?

A Fly trap.
B Intruder alarm server.
C DMZ proxy.
D Honeypot.

3 What type of firewall inspects packets to identify VALID communications?

A Stateful inspection.
B Intrusion prevention.
C Intrusion detection.
D Application layer.

4 What is the process called which allows all activities on a network to be traced to the user who performed them?

A Verification.
B Authorisation.
C Accountability.
D Identification.

5 Which of the following statements is TRUE?

A All malware are viruses.
B Not all viruses are malware.
C All viruses are malware.
D All adware is malware.

6 What type of security threat replicates itself, by using a client’s list of email addresses and then forwarding itself to all of them?

A Logic bomb.
B Virus.
C Trojan horse.
D Worm.

7 Which acronym which describes the duration after which an organisation's viability will be permanently threatened, if product and service delivery **CANNOT** be resumed?

A RTO.
B RPO.
C MTTR.
D MTPOD.

8 Which type of attack is only concerned with consuming bandwidth and resources on the target network and **USUALLY** uses IP spoofing?

A Man-in-the-middle.
B Denial of service.
C Hacking.
D Social engineering.

9 Which protocol can automatically provide the IP address, subnet mask, default gateway IP and DNS server IP to a client on a data network?

A RPC.
B ARP.
C DHCP.
D DNS.

10 An attacker hacks a DNS server and changes a company's web server IP address to a spoofed website. What is this type of activity called?

A DNS alias.
B DNS forwarding.
C DNS poisoning.
D DNS round robin.

11 Which feature prevents infected files being installed on a device?

A Driver signature enforcement.
B User Account Control.
C BitLocker.
D AppLocker.

12 Which of the following is native to Microsoft?

A IPsec.
B EFS.
C 802.1x.
D AES.

13 A firewall denies traffic on ports 20 and 21. Which protocol is **NOT** allowed through?

A DHCP.
B FTP.
C TFTP.
D DNS.

14 A network engineer monitors a firewall and notices several suspicious packets have been dropped. What is in place on the firewall?

A IDS.
B Proxy filtering.
C IPS.
D ARP.

15 Which of the following protocols is used as a security protocol and is also one of the secure encryption systems used in data communication?

A SMTP.

B Kerberos.

C TFTP.

D DNS.

16 Which is the CORRECT group policy processing order?

A Local, site, domain, OU.

B Domain, site, OU, local.

C Site, OU, local, domain.

D Local, domain, site, OU.

17 Which type of tool is used to find modems on networks to initiate an attack from?

A Virus scanner.

B Port scanner.

C War dialler.

D Easter egg.

18 A firewall router can hide the company IP addresses behind another IP address, providing some level of security. What is this feature called?

A Stateful inspection (SI).

B Network address translation (NAT).

C Demilitarised zone (DMZ).

D Orange zone (OZ).

19 You are asked to set up a system to analyse local network traffic for suspicious activity and send notifications when a possible attack is taking place. What **SHOULD** be done?

A Install a network-based IDS.

B Install a host-based IDS.

C Install a network-based honeypot.

D Set up verbose logging on the firewall.

20 Which file system allows file and folder permissions to be configured on Windows systems?

A FAT32.
B XFS.
C NTFS.
D FAT16.

-End of Paper-