Making IT
good for
society

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

Sample Paper A

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

Sample paper only 40 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 26/40.

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.

21 What does OS hardening mean?

A Improving security by adding anti-malware protection.

B Removing unnecessary software, profiles and services.

C Defragmenting the hard disk to better use the space.

D Updating the BIOS to increase protection.

22 What is happening if a firewall permits / denies traffic based on port number?

A Application filtering.

B Stateful inspection.

C Packet filtering.

D Stateful multi-layer inspection.

23 When installing a new system, at what stage **SHOULD** protection against malicious software be installed?

A After system updates.

B It does not matter.

C Once the rest of the software has been installed.

D Immediately after installing the operating system.

24 Which of the following is an example of an asymmetric algorithm?

A 3DES.

B AES.

C RSA.

D Blowfish.

25 Which protocol would be set up as a secure alternative to Telnet during commissioning?

A SSH.
B FTPS.
C HTTP.
D SCP.

26 A company is concerned about social engineering and has asked what can be done to mitigate the threat. What would be the **BEST** recommendation?

A Update the anti-virus software.
B Install biometric access doors at the computer room.
C Upgrade to a three stage application firewall.
D User awareness and training.

27 A network engineer is working on a helpdesk when a call is received from an administrator at a remote office, who claims to have forgotten the root password for a server. What kind of attack might be taking place?

A War dialling attack.
B Brute force attack.
C Social engineering attack.
D Man-in-the-middle.

28 What type of firewall keeps track of TCP and UDP connections?

A Application level.
B Host.
C Packet filter.
D Stateful.

29 SYN flooding is a type of what?

A Virus replication.
B Trojan horse.
C Password cracking attack.
D Denial of service attack.

30 What is it called when a person slips through an open door behind an employee, which may lead to a security breach?

A Horseback riding.
B Gliding.
C Tailgating.
D Slithering.

31 Which file transfer protocol uses UDP as a transport protocol and lacks security?

A FTP.
B TFTP.
C SFTP.
D RPC.

32 By default, what is the minimum number of characters for a password in a Windows Server 2012 installation?

A Five.
B Six.
C Seven.
D Eight.

33 A virus has been detected on a device connected to a network. What **SHOULD** be done first?

A Update the anti-virus software.
B Contact the user to let them know what has happened.
C Disconnect the device from the network.
D Run a virus scan on all shared areas.

34 A network engineer is instructed to prevent USB use on Windows based devices used in the Finance department. Which of the following would be the **BEST** solution?

A Uninstall USB drivers from all Finance devices.
B Add a group policy to all users in Finance.
C Add a group policy to the Finance group.
D Install physical USB locks to Finance devices.

35 What is the security principle called where users are only given the rights necessary for them to perform their jobs?

A Least privilege.
B Role-based access.
C Duty correlation.
D Functional permissions.

36 What is the name of a program that claims to be one thing but in fact contains malicious code?

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

37 Which device can supply backup power to a PC when the electricity fails?

A UPS.
B SPS.
C Line conditioner.
D Surge suppressor.

38 Which Microsoft security feature is designed to prevent unauthorised changes to the system?

A AppLocker.
B BitLocker.
C User Account Control.
D Advanced firewall.

39 What is the term used when phishing attacks are targeted towards a particular person, such as an executive, in a company?

A Phreaking.
B Sharking.
C Probing.
D Whaling.

40 Which combination of permissions apply to a folder on a remotely accessed device in a Windows network?

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

-End of Paper-