BCS Level 4 Certificate in Security Technology Building Blocks
QAN 603/0884/9

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.

This qualification is regulated by Ofqual (in England).

1 Which of the following statements is TRUE for the process of mutual authentication?

A Two remote systems authenticate each other at the same time.
B Two remote systems authenticate each other in sequence.
C Three or more remote systems authenticate each other at the same time.
D Three or more remote systems authenticate each other in sequence.

2 Which of the following is a feature of symmetric encryption?

A Only the recipient must know the secret key.
B The keys can safely be published online.
C Two keys exist, one to encrypt the message, the other to decrypt the message.
D The same key is used to decrypt and encrypt.

3 Which of the following is **LEAST LIKELY** to be placed in a corporate DMZ?

A Web servers.
B FTP servers.
C Database servers.
D Mail servers.

4 Security SHOULD first become involved in which stage of the application development life cycle?

A Prior to the implementation of the application.
B Prior to user acceptance testing.
C During unit testing.
D During requirements development.

5 What is the **BEST** practice when installing anti-virus updates?

A Update as soon as possible.
B Wait to get feedback first about the update.
C It is working fine as it is, update in the future.
D Wait 3 months to make sure that there are no bugs.

6 Which of the following is an example of social engineering?

A Sending an email with a malicious link attached requesting information to be added.
B Sending an email and offering to pay for an organisations data.
C Sending an email demanding your personal details be removed from a data list.
D Sending an email to return sensitive information you have been sent.

7 An application fails to error check input between data or code. Which OWASP Top 10 vulnerability is **MOST LIKELY** to occur in the application?

A Injection Attack.
B Insecure direct object references.
C Failure to restrict URL access.
D Insufficient transport layer protection.

8 A security administrator is evaluating various firewalls to find the best solution for an office environment with an email server. Which of the following is an undesirable feature of a firewall in this environment?

A Only specified traffic can be allowed to pass through.
B The firewall itself should be immune to penetration.
C It should allow for configuration changes by authorised users.
D It must only allow network traffic to travel from inside the network to the Internet.

9 Which one of the following is **GENERALLY** a poor practice for managing passwords?

A Passwords should be changed once in 5 years.
B Users must change their passwords at their first login.
C It contains upper and lower-case characters.
D It contains numbers and special characters.

10 What term is used where an organisation selectively defines the path that certain packets take through their network?

A Dynamic routing.
B Static routing.
C Policy-based routing.
D Snapshot routing.

11 Which three of the following **SHOULD** the security administrator implement to limit web traffic based on country of origin?

a) Spam Filter.
b) Load Balancer.
c) Antivirus.
d) Proxies.
e) Firewall.
f) NIDS.
g) URL Filtering.

A a, b and g only.
B d, e and f only.
C c, f and g only.
D a, b and e only.

12 Which of the following are suitable for a secure transfer of data?

A SSL and TELNET.
B SSH and SFTP.
C SFTP and TELNET.
D None of these.

13 Biometric authentication, electromagnetic shielding and advanced locking mechanisms are **TYPICALLY** used as security in which OSI Layer?

A Network.
B Physical.
C Transport.
D Presentation.

14 An example of a system that is able to control access to network resources, enforce policies and supply the information necessary to bill for services is?

A An intrusion detection system.
B A stateful firewall.
C A RADIUS server.
D An intrusion protection system.

15 What is the purpose of a hash function in a secure exchange of messages over open networks?

A It secures data from an attack by an eavesdropper.
B It allows a user to check if the original data has been tampered with.
C It encrypts the data to prevent reading by unauthorised users.
D It creates a secure digital envelope for data.

16 A system having INCORRECT permissions set on files, folders, and symbolic links has which of the following?

A Vulnerabilities.
B Threats.
C Risks.
D Exploits.

17 You are setting up a single sign-on authentication system for a large enterprise LAN containing 5000 users. Which of the following authentication protocols would be **MOST** appropriate?

A SAML.
B XACML.
C SASL.
D Kerberos.

18 Select the **MOST** significant concern to an organisation when storing data across a cloud provider's network which is geographically distributed?

A It has data sovereignty concerns for the stored data across geo-political locations.
B Network latency between sites may increase.
C Confidentiality of the stored data is an increased security concern.
D Data recovery becomes harder due to accessibility issues across multiple gro-political locations.

19 Which of the following accreditation bodies in the UK run an accreditation process for organisations providing penetration testing?

A CREST (The Council for Registered Ethical Security Testers).
B EC Council.
C ISC2 (International Information System Security Certification Consortium).
D ISACA (Information Systems Audit and Control Association).

20 Which of the following is a characteristic of a RADIUS system?

A It is a hardened file access system.
B It operates at the Transport layer to identify duplicate network segments.
C It provides centralised Triple A management for users who connect and use a network service.
D It provides centralised encryption for network traffic and alerts the network administrator of unauthorised eavesdropping.

21 What type of authentication system requests a username, a password and requires the user to type the code displayed on a disconnected token generator?

A Message.
B Double.
C Complex.
D Two-factor.

22 Why is it good practice for an organisation to place a shredder next to a network printer?

A To encourage employees to securely destroy all unwanted prints.
B So that misprints can be easily disposed of by employees.
C To encourage employees to recycle unwanted copies.
D To keep the print room tidy and safe from slip hazards.

23 Which of the following describes a Zero-day software vulnerability?

A It is considered as a low priority business risk by developers and vendors.
B It is known to the vendor as an auxiliary non-critical information.
C It is not known to the vendor until it is exploited by hackers.
D It is exploitable by the tech savvy employees working for the vendor.

24 What is the importance of patching-up security issues of antivirus software?

A To prevent vulnerabilities from being exploited.
B To comply with company maintenance schedule.
C To ensure all software code is unaffected.
D To comply with licencing agreements.

25 Which of the following methods is likely to produce the **LEAST** problems in password management by employees?

A Enforcing password changes every month.
B Allowing staff to choose their own passwords.
C Issuing centrally-assigned passwords.
D Training staff to use mnemonic-based passwords.

26 Which risk mitigation technique is used to counter the threat of repudiation?

A Installing load balancers.
B Using a strong encryption.
C Prompt system patching.
D Enabling system auditing.

27 What term is applied to a physical or logical subnetwork that exposes an organisation's external facing servers to an untrusted network, such as the Internet?

A Corporate Server Zone (CSZ).
B Reverse Proxy Zone (RPZ).
C Unrestricted Zone (URZ
D Demilitarised Zone (DMZ).

28 An organisation would use a demilitarised zone (DMZ) to avoid exposure of which of the following?

A Its computers to the internet.
B Its computers to the firewall.
C Its firewall to the Internet.
D The Internet to its business processes.

29 Which of the following responses accurately describes Payment Card Industry Data Security Standard (PCI DSS) compliance?

A An organisation can guarantee that credit card and financial data will never be lost.
B An organisation has followed the rules set forth in the PCI DSS standard and can offer proof in the form of documentation.
C An organisation is not liable if credit card or other personal data is lost or stolen.
D An organisation does not store PAN or CVV data under any circumstances.

30 Which of the following is **NOT** a benefit of implementing Virtual LANs (VLAN) within a network?

A Reduced broadcast traffic.
B Greater network segregation.
C Enhanced security policy enforcement.
D Lower administrative overhead.

31 During a network DDoS attack, implementation of which of the following controls is **MOST LIKELY** to support network availability?

A IP address blacklisting.
B Hardware based load balancers.
C IP address whitelisting.
D Web Application Firewall (WAF).

32 Which of the following provides the **BEST** increase in integrity when implementing a Full Disk Encryption (FDE) solution for an end-user laptop?

A Trusted Platform Module (TPM).
B Hardware Security Module (HSM).
C Public Key Infrastrcuture (PKI).
D Advanced Encryption Standard (AES).

33 Which of the following is **GENERALLY** considered as the **MOST** secure identification technology?

A Biometrics.
B Barcode cards.
C Personal Identification Numbers (PINs).
D One-time passwords.

34 Which type of proxy server retrieves resources on behalf of a client from one or more servers?

A Open.
B Reverse.
C Trans.
D SOCKS.

35 Parameterised queries in SQL are used to protect databases against which type of attack?

A Operating system vulnerabilities.
B Unauthorised privilege elevation.
C Privilege abuse.
D SQL injection.

36 What type of access control is implemented where a database administrator can grant UPDATE privileges in a database to specific users or groups?

A Supplemental.
B Discretionary.
C Mandatory.
D System.

37 According to the SANS Top 20 Critical Security Controls for Effective Cyber Defence, which of the following is **NOT** a critical security control?

A Physical protection.
B Data protection.
C Boundary defence.
D Malware defence.

38 What is the purpose of DMZ?

A To act as an additional security level for a switch.
B To act as an additional security level for a router.
C To allow two trusted networks to operate securely without a firewall.
D To add an additional layer of security to a local area network (LAN).

39 Which type of penetration testing provides the **MOST** realistic assessment of a real-world attack by an external threat actor?

A Black box.
B Orange box.
C White box.
D Grey box.

40 When designing a secure login portal for a website, which of the following control combinations provides the **BEST** confidentiality, integrity and availability?

A Single-factor authentication, HTTP and stateful firewall.
B Multi-factor authentication, HTTPS and Web Application Firewall (WAF).
C Single-factor authentication, HTTPS and layer 2 firewall.
D Multi-factor authentication, HTTPS and stateful firewall.

-End of Paper-