Making IT good for society

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

Specimen Paper A

Record your surname/ last/ family name and initials on the Answer Sheet.

Specimen paper only. 20 multiple-choice questions – 1 mark awarded to each question. Mark only one answer for 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.

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 What does the below statement perform?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

A Buffer overflow prevention.
B Input validation.
C Cross-site request forgery prevention.
D SQL injection prevention.

3 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.

4 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.

5 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.

6 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.

7 Which of the following is **UNLIKELY** to be included in a SLA?

A The types of issues are excluded.
B The response time to incidents.
C The cost to resolve the incident.
D The percentage of uptime expected.

8 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.

9 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).

10 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.

11 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.

12 In which phase of a penetration test **SHOULD** a security analyst perform scanning?

A Pre-attack.
B Attack.
C Post-attack.
D Reconnaissance.

13 How **SHOULD** an enterprise impose security requirements on their contractors?

A Meeting with the contractor on a regular basis.
B By defining staff training needs.
C By regularly attacking the contractor's network.
D By defining security policy in the SLA.

14 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.

15 Which HTTPS port is **MOST** commonly used to secure websites?

A 22
B 443
C 500
D 706

16 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.

17 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.

18 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.

19 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).

20 How does AIDC work?

A It automatically converts an image or a sound into a digital file.
B It identifies and captures data to enable manual conversion to a file.
C It will isolate data capture from security threats.
D It automatically identifies and detects computers IP addresses.

-End of Paper-