Level 3 Technical Level

IT: CYBER SECURITY

Unit 6   Network and cyber security administration

Friday 15 June 2018 — Afternoon — Time allowed: 2 hours

Materials

For this paper you may use:
- a ruler
- a scientific calculator (non-programmable)
- stencils or other drawing equipment (eg flowchart stencils).

Instructions
- Use black ink or black ball-point pen.
- Fill in the boxes at the top of this page.
- Answer **all** questions.
- You must answer each question in the space provided. Do not write outside the box around each page or on blank pages.
- Do all rough work in this book. Cross through any work you do not want to be marked.
- If you need more space use the additional pages at the back of this booklet.

Information
- The marks for questions are shown in brackets.
- The maximum mark for this paper is 80.
- There are 50 marks for **Section A** and 30 marks for **Section B**. Both sections should be attempted.

Advice
- In all calculations, show clearly how you work out your answer.
- Use diagrams, where appropriate, to clarify your answers.
- You are expected to use a calculator where appropriate.
- You are reminded of the need for good English and clear presentation in your answers.

For Examiner's Use	
Question	Mark
1–5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
TOTAL	

J/507/6435

Section A

Answer **all** questions in this section.

In multiple choice questions, only **one** answer per question is allowed.

For each answer completely fill in the circle alongside the appropriate answer.

CORRECT METHOD   ●   WRONG METHODS   ⊗ ◉ ⬭ ⊘

If you want to change your answer you must cross out your original answer as shown.   ⊠

If you wish to return to an answer previously crossed out, ring the answer you now wish to select as shown.   ⊗

You may do your working in the blank space around each question but this will not be marked. Do **not** use additional sheets for this working.

0	1		Which **one** of the following is a characteristic of 'ransomware'?

[1 mark]

A   provides the user with some benefit   ⬭

B   removes vulnerabilities from a computer   ⬭

C   encrypts files on a computer   ⬭

D   secretly records user interaction   ⬭

0	2		Which **one** of the following is not an Information Technology Infrastructure Library (ITIL) volume?

[1 mark]

A   ITIL Service Strategy   ⬭

B   ITIL Service History   ⬭

C   ITIL Service Operation   ⬭

D   ITIL Service Transition   ⬭

0 3   Which of the following does a digital signature usually require?

[1 mark]

A   a public key ⬯

B   a key generating algorithm ⬯

C   a private key ⬯

D   all of the above ⬯

0 4   The Computer Misuse Act 1990 protects individuals and businesses from data loss. What is the maximum penalty for offences under this Act?

[1 mark]

A   a Fixed Penalty Notice ⬯

B   extradition to the USA ⬯

C   imprisonment and a fine ⬯

D   £5000 fine ⬯

0 5   Which **one** of the following best describes a Denial of Service attack?

[1 mark]

A   a user's permission to access to services is withdrawn ⬯

B   a user is prevented from accessing files on their home computer ⬯

C   an intentional attempt to overload a network resource ⬯

D   a legitimate reduction of service ⬯

5

Turn over ▶

0 6 A sudden power cut could cause complete loss of data stored in computer memory.

0 6 . 1 State **two** ways of preventing loss of data when there is a power cut.

[2 marks]

1 _____

_____

2 _____

_____

0 6 . 2 Cloud storage and DVD are two methods of backing up data.

State **one** disadvantage of each method.

[2 marks]

Cloud storage _____

_____

DVD _____

_____

4

0 7 . 1 What type of data was covered by the Data Protection Act?

[1 mark]

_____

_____

0 7 . 2 State **one** principle of the Data Protection Act.

[1 mark]

_____

_____

0 7 . 3 In May 2018, the General Data Protection Regulation (GDPR) replaced the Data Protection Act.

State **two** ways the need for consent underpins the GDPR.

[2 marks]

1 _____

_____

2 _____

_____

4

0 8 Explain how an office cleaner could help to mount a cyber attack on a company.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

_____

4

Turn over for the next question

Turn over ▶

0 9 Encryption is used to protect information. Usually encryption is a good thing.

0 9 . 1 Describe a situation where encryption might be a problem.

[2 marks]

_____

_____

_____

_____

0 9 . 2 Some politicians have talked about banning encryption.

Explain what problems this might cause.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

_____

6

1 0 . 1 Describe what is meant by an 'agitation campaign'.

[2 marks]

_____

_____

_____

_____

1 0 . 2 How might an agitation campaign work on Twitter or Facebook?

[1 mark]

_____

_____

3

1 1 In the USA, TEMPEST was a National Security Agency programme that involved the monitoring (and shielding) of devices that unintentionally emit signals called 'leaking emanations'.

Give **two** examples of 'leaking emanations'.

[2 marks]

1 _____

2 _____

2

Turn over for the next question

Turn over ▶

1 2 Penetration testing is an authorised attempt to find vulnerabilities in a network that an attacker could exploit.

1 2 . 1 Explain what is meant by the 'scope' of a penetration test.

[4 marks]

_____

_____

_____

_____

_____

_____

1 2 . 2 Describe **two** ways a penetration test is different from a vulnerability scan.

[4 marks]

1 _____

_____

_____

2 _____

_____

_____

8

Do not write outside the box

1 3 . 1 Explain, giving examples, the difference between 'authentication' and 'access control'.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

_____

1 3 . 2 Describe **two** examples of access control security models.

[4 marks]

1 _____

_____

_____

_____

2 _____

_____

_____

_____

8

Turn over ▶

14 . 1 Describe the CHECK assurance scheme.

[2 marks]

_____

_____

14 . 2 Name **two** types of organisation that use the CHECK assurance scheme.

[2 marks]

1 _____

_____

2 _____

_____

14 . 3 List **two** principles of CHECK membership.

[2 marks]

1 _____

_____

2 _____

_____

6

Do not write outside the box

Section B

Answer **all** questions in this section.

| 1 | 5 |

The Trusted Computing Base (TCB) of a system is critical to its security.

| 1 | 5 | . | 1 |

Name the **three** components of a TCB.

[3 marks]

1 _____

2 _____

3 _____

| 1 | 5 | . | 2 |

Explain how the design and implementation of a system's TCB affects its overall security.

[3 marks]

_____

_____

_____

_____

_____

_____

Question 15 continues on the next page

Turn over ▶

Do not write outside the box

15.3 The WannaCry ransomware attack in May 2017 targeted computers running the Windows operating system, including many in the NHS in England.

Discuss reasons why the NHS computer network might have been vulnerable to an attack.

[9 marks]

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

15

1 6 Steganography is an anti-forensic method, where a file is hidden in another file, as a way of avoiding data detection.

1 6 . **1** Name **three** other locations in a computer system where data could be hidden.

[3 marks]

1 _____

2 _____

3 _____

1 6 . **2** Explain methods that computer forensic analysts use to collect and preserve digital evidence.

[12 marks]

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

15

Extra space available on the next page if required

Turn over ▶

END OF QUESTIONS

If needed, use the following pages to continue your answers. Write the question number beside your answer.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Turn over ▶

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____