Please write clearly in block capitals.

Centre number ☐☐☐☐☐   Candidate number ☐☐☐☐

Surname _____

Forename(s) _____

Candidate signature _____

Level 3 Technical Level

IT: NETWORKING
Unit 6   Network security management

Wednesday 13 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	
17	
18	
19	
20	
TOTAL	

Do not write outside the box

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 would you **not** expect to find in a VPN (Virtual Public Network) policy? |

[1 mark]

A privileges to ensure unauthorised users are denied access ◯

B controls on the use of split tunnelling ◯

C automated forwarding of email to external destinations ◯

D evaluation of risk and determining control measures ◯

| 0 | 2 | Which legislation made it illegal to use other people's broadband connection without permission? |

[1 mark]

A Communications Act (2003) ◯

B Small Business, Enterprise and Employment Act (2015) ◯

C Computer Misuse Act (1998) ◯

D Investigatory Powers Act (2016) ◯

Do not write outside the box

| 0 | 3 | Which **one** of the following is **not** an aim of penetration testing?

[1 mark]

A minimising risk by identifying vulnerabilities and blocking threats ⬭

B modelling real-world threats to discover vulnerabilities ⬭

C controlled exploitation to discover business risk ⬭

D using a vulnerability to cause damage to a target system ⬭

| 0 | 4 | In which **one** of the following sections would you expect to find 'objectives' in a Network Security Plan?

[1 mark]

A assessment results ⬭

B overview ⬭

C resources and budget ⬭

D appendix ⬭

| 0 | 5 | Which **one** of the following is **not** an encryption or security protocol?

[1 mark]

A TKIP ⬭

B VPN ⬭

C WPA2 ⬭

D WEP ⬭

| | 5 |

Turn over ▶

4

0 6 Organisations should scan their systems regularly for vulnerabilities. Scanning is one way of identifying weak points in a network.

Suggest why vulnerability scanning should be continuous and automated.

[2 marks]

_____

_____

_____

_____

2

0 7 'Never open an attachment directly from email.'

Opening an attachment directly from email is something the vast majority of IT users do every single day.

Explain why this may prove harmful to your PC, laptop or network.

[2 marks]

_____

_____

_____

_____

2

0 8 One way of securing a network is through a Wireless Intrusion Prevention System (WIPS).

Give **one** threat that a WIPS might identify, and **one** response that a WIPS might provide.

[2 marks]

_____

_____

_____

_____

2

Do not write outside the box

0 9   Suggest **two** disciplinary actions you might find in a Computer Acceptable Use Policy.

[2 marks]

1 _____

_____

2 _____

_____

2

1 0   Sending commercially sensitive data wirelessly to other equipment is now common practice.

1 0 . 1   Wi-Fi Protected Access (WPA) is a security standard or protocol.

What is meant by a security standard or protocol?

[1 mark]

_____

_____

1 0 . 2   Wi-Fi Protected Access (WPA) replaced and improved upon Wired Equivalent Privacy (WEP).

Give **two** areas where improvements have been made.

[2 marks]

1 _____

_____

2 _____

_____

3

Turn over ▶

Do not write outside the box

1 1 Many people now access bank accounts through their mobile phones.

Explain recent improvements in authentication techniques used to secure accounts.

[3 marks]

_____

_____

_____

_____

_____

_____

3

1 2 In developing a Network Security Plan, you would review, classify, and prioritise business critical assets and exposures.

1 2 . 1 Give **three** examples of content you might include.

[3 marks]

1 _____

_____

2 _____

_____

3 _____

_____

1 2 . 2 Risk assessments help determine which assets are at greatest risk.

Give **three** issues that a risk assessment should consider.

[3 marks]

_____

_____

_____

_____

_____

_____

6

Do not write outside the box

1 3 Explain what the role of an ethical hacker might involve.

[3 marks]

_____

_____

_____

_____

_____

_____

3

1 4 Logs are used to routinely monitor a network.

1 4 . 1 State **two** items that might be monitored or logged.

[2 marks]

1 _____

_____

2 _____

_____

1 4 . 2 Explain why monitoring or logging is undertaken, providing examples of what might cause concern or need further investigation.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

6

Turn over ▶

1 5   For a Security Service Level Agreement (SSLA) to be meaningful, it must define criteria capable of being measured.

State **three** criteria appropriate for measuring performance and explain how each might be measured.

[6 marks]

1 _____

_____

_____

_____

2 _____

_____

_____

_____

3 _____

_____

_____

_____

6

1 6   Explain how a packet sniffer works.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

4

Do not write
outside the
box

1 7 Continuous Network Security Monitoring (CNSM) helps an organisation to maintain awareness of vulnerabilities and threats.

Network Security Managers often refer to front end security and back end security in the context of CNSM.

Explain the terms front end security and back end security in this context.

[6 marks]

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

6

Turn over for the next question

Turn over ▶

0 9

Do not write outside the box

Section B

Answer **all** questions in this section.

| 1 | 8 | You are a Network Manager reviewing an in-house **Security Service Level Agreement (SSLA)** that is managed by colleagues within your own department. |

| 1 | 8 | . | 1 | As part of your review, you find reference to email abuse has been limited to viruses and malware. |

List **four** forms of email abuse that are not classified as viruses.

[4 marks]

_____

_____

_____

_____

_____

_____

| 1 | 8 | . | 2 | Your virus detection Service Level Agreement (SLA) for email security will not offer 100% protection. |

Explain when, either due to employee action or inaction your SLA for email security will not apply.

[4 marks]

_____

_____

_____

_____

_____

_____

_____

8

Do not write outside the box

1 9 Breaches in network security can have severe consequences for organisations. The **Computer Misuse Act (1990)** is designed to protect computer users against deliberate attacks and the theft of information.

State **three** offences identified in this Act and discuss why some actions would attract more severe penalties than others.

[7 marks]

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

7

Turn over for the next question

Turn over ▶

Do not write
outside the
box

2 **0** Authentication, authorisation, and access control all contribute to network security.

Explain how network security is achieved.

In your answer you should:

- define authentication, authorisation, and access control
- give a suitable example of each one
- and, for each one, explain how network security is achieved.

[15 marks]

Do not write outside the box

15

END OF QUESTIONS

Turn over ▶

Do not write outside the box

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

There are no questions printed on this page

DO NOT WRITE ON THIS PAGE
ANSWER IN THE SPACES PROVIDED

Do not write outside the box