AQA

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

Friday 25 January 2019 Morning Time allowed: 2 hours

Materials

For this paper you must have:

- 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	
TOTAL	

Section A

Answer **all** questions in this section.

0 1 Email authentication provides information about the

Tick (✓) **one** box.

[1 mark]

attachment or number of attachments. □

recipient or number of recipients. □

sender or origin of an email. □

size of email or size limitation of email server. □

0 2 Which of the following will be found within a network-layer firewall?

Tick (✓) **one** box.

[1 mark]

application shield □

input validation □

packet filtering □

VPN encryption □

0 3 DNS (Domain Name Service) spoofing will attempt to

Tick (✓) **one** box.

[1 mark]

change the factory-assigned MAC address. □

intercept data frames on a network. □

link the attacker's MAC address with a false IP address. □

redirect users to a different computer. □

0 4 Which of the following defines a honeynet?

Tick (✓) **one** box.

[1 mark]

a network set up to invite attack. □

a part of a honeypot. □

a server probing for open ports. □

an inventory of systems and services. □

Turn over for the next question

0 5 Which of the following describes an Acceptable Use Policy?

Tick (✓) **one** box.

[1 mark]

a list of ethical hacking techniques. □

circumstances when an employer can access personal email accounts. □

guidance for reposting copyrighted material without permission. □

the rules a user must accept before accessing a network. □

5

0 6 Define the term polymorphic malware.

[1 mark]

1

0 7 . 1 Give **one** feature of symmetric encryption.

[1 mark]

0 7 . 2 Give **one** feature of asymmetric encryption.

[1 mark]

2

0 8 Event logs and audit logs are tools a network manager uses to monitor their network.

0 8 . 1 Describe how a network manager uses an event log to monitor network activity.

[4 marks]

0 8 . 2 List **two** items you would expect to find in an audit log used to monitor a network.

[2 marks]

1 __________

2 __________

6

0 9 A protocol analyser is also known as a network analyser or network packet analyser.

0 9 . 1 Give **one** method a protocol analyser uses to monitor a network.

[1 mark]

0 9 . 2 Name **one** other type of protocol analyser.

[1 mark]

2

Turn over for the next question

1 0 A network manager can use penetration testing and vulnerability assessments to test the security of their network.

1 0 . 1 Define vulnerability assessment.

[1 mark]

1 0 . 2 Describe **two** threats vulnerability assessments might miss**.**

[4 marks]

1

2

1 0 . 3 Explain what penetration testing aims to achieve.

[3 marks]

1 0 . 4 Explain why continuous network security monitoring (CNSM) has **not** replaced all use of vulnerability assessments and penetration testing.

[2 marks]

10

Turn over for the next question

1 1 Some organisations exchange data with their suppliers and customers.

Intrusion prevention and detection systems should be in place.

1 1 . 1 List **two** other elements of basic perimeter security you would expect any organisation to have.

[2 marks]

1 ______________________________

2 ______________________________

1 1 . 2 Explain why an organisation should also look at the systems of suppliers and customers when considering network security monitoring.

[4 marks]

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

6

1 2 All organisations should have network security policies.

1 2 . 1 Explain why an organisation needs a Wireless Communications Policy.

[2 marks]

1 2 . 2 Describe what a Remote Access Policy might cover.

[2 marks]

1 2 . 3 Explain why an Automatically Forwarded Email Policy might apply to a business email account but **not** to an employee's personal email account.

[2 marks]

6

Turn over for the next question

Do not write outside the box

1 3 A Service Level Agreement (SLA) is one way a client and provider can improve communications, manage expectations, and clarify responsibilities.

Describe **three** steps necessary for client and provider to develop an SLA if the final agreement is to work well for both.

[6 marks]

1 ______________________________

2 ______________________________

3 ______________________________

6

1 4 A Network Security Plan should cover all aspects of an organisation's network security. The plan should provide management with all the information needed to maintain a secure network. The plan will be monitored and reviewed.

Name **three** sections you would expect to find listed on the contents page of an organisation's Network Security Plan.

Describe **one** item you would find included in each of your three named sections.

[6 marks]

Section 1 ____________________

Item ____________________

____

____

Section 2 ____________________

Item ____________________

____

____

Section 3 ____________________

Item ____________________

____

____

6

Turn over for Section B

Section B

Answer **all** questions in this section.

1 5 Network security systems should ensure only trusted users and devices gain access. Detecting intrusion and raising the alarm is an important part of any network security system.

Most organisations have an Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS).

Discuss how these two systems contribute to a network security system.

Give examples in your answer.

[9 marks]

Do not write outside the box

9

Turn over for the next question

1 6 Network access control (NAC) restricts resources to approved users and devices, but works only inside the perimeter. Once users are verified they have wide-ranging network access. NAC has been described as ‘old technology’.

Discuss how NAC protects a network. You should include:

- how NAC secures access to a network
- how effective NAC is
- whether ‘next generation’ NAC protects a network more effectively.

[9 marks]

Turn over for the next question

9

1 7 A network security manager has to determine threats, vulnerabilities and risks.

1 7 . 1 Explain the difference between an exposure and an exploit.

Give examples in your answer.

[6 marks]

1 7 . 2 A threat has the potential to cause harm. A risk is the likelihood of a threat becoming a reality and the loss or impact it would have if successful.

Describe the impact an unhappy and angry employee might have on an organisation's systems.

[6 marks]

12

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.

Do not write outside the box

There are no questions printed on this page

DO NOT WRITE ON THIS PAGE
ANSWER IN THE SPACES PROVIDED

Copyright information