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

Wednesday 24 January 2018 Morning Time allowed: 2 hours

Materials
For this paper you must have:
- a ruler.

You may use:
- 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 the questions in the spaces 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.

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**.
- There are **two** sections to this paper.
- Both sections should be attempted.
- Candidates should spend approximately 60 minutes on **Section A** and 30 minutes on **Section B**.

Advice
- Please read each question carefully before starting.
- 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	
Examiner's Initials	
Question	Mark
1–5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
TOTAL	

Do not write outside the box

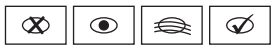
Section A

Answer **all** questions in this section.

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

For each question 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. 

0 1 Which of the following provides a definition of **shellcode**?

A A general purpose programming language. ⬭

B An object-oriented programming language. ⬭

C Hexidecimal instructions a computer responds to directly. ⬭

D A small piece of code used to exploit software vulnerability. ⬭

[1 mark]

1

0 2 An **authentication protocol** has been described as the most important layer of protection needed for secure communication. Point-to-point protocols (PPP) are used to authenticate communications.

Which of the following is a Point-to-Point (PPP) protocol?

A Password Authentication Protocol (PAP). ⬭

B Transmission Control Protocol (TCP). ⬭

C Border Gateway Protocol (BGP). ⬭

D File Transfer Protocol (FTP). ⬭

[1 mark]

1

Do not write outside the box

0 3 A client-side attack may result if

A an Xpath query accesses the database server. ⬭

B network traffic is not permitted. ⬭

C client applications interact with a malicious server. ⬭

D a web server prevents legitimate use of a service. ⬭

[1 mark]

1

0 4 Public-key cryptography (PKC) requires

A a public key and a private key. ⬭

B the same algorithm and key. ⬭

C interchangable keys. ⬭

D one-way encryption. ⬭

[1 mark]

1

0 5 The **Data Retention (EC Directive) Regulations (2009)** controls

A access to a computer without permission. ⬭

B offensive and threatening messages. ⬭

C the sending of electronic marketing messages. ⬭

D how data is acquired and stored. ⬭

[1 mark]

1

Do not write outside the box

0 6 State **one** way in which a denial-of-service attack (DoS attack) is different from a distributed denial of service attack (DDoS attack).

[1 mark]

1

0 7 Malware is an abbreviation meaning 'malicious software'. Both spyware and adware are forms of malware.

Explain why spyware may have more serious consequences than adware.

[2 marks]

2

0 8 Explain why **spear phishing attacks** are far more likely to succeed than traditional phishing attacks.

[2 marks]

2

0 9 Wi-Fi Protected Access (WPA) provided an improvement to Wired Equivalent Privacy (WEP). Until then, WEP had been the most widely used Wi-Fi security protocol in the world.

State **two** security improvements WPA2 provides compared with WPA.

[2 marks]

1 _____

2 _____

2

Do not write outside the box

1 0 A firewall is an example of perimeter security.

1 0 . 1 Give another example of **perimeter** security.

[1 mark]

_____

_____

1 0 . 2 Even if your client's perimeter systems are fully up to date, new attacks will still get through.

Using the **layered-security model**, give **one** example of added protection under each of the following headings:

[3 marks]

Network _____

_____

Host _____

_____

Data _____

_____

4

1 1 Access control is a security technique used to regulate who or what can view or use resources in a computing environment.

List **four** examples of access control.

[4 marks]

1 _____

_____

2 _____

_____

3 _____

_____

4 _____

_____

4

Turn over ▶

Do not write outside the box

1 2 It is unlikely that any business could prevent all attacks and their Network Security Manager's aim will be to detect attacks as effectively and efficiently as possible. Continuous monitoring is often preferred to scheduled or periodic monitoring.

There are three distinct phases of **continuous network security monitoring (CNSM)**, these are plan, monitor and action.

For each phase, describe **one** activity you might complete and what you would hope to achieve in doing so.

[6 marks]

Plan _____

_____

_____

_____

Monitor _____

_____

_____

_____

Action _____

_____

_____

_____

6

Do not write outside the box

1 3 A Service Level Agreement (SLA) is a contract between a customer and a service provider defining the level of service expected.

1 3 . 1 Provide an example or explanation of what might be included for each of the **four** elements listed below.

[4 marks]

Responsibilities _____

_____

Expectations _____

_____

Penalties _____

_____

Incentives _____

_____

1 3 . 2 Give **two** potential benefits of a business having a service level agreement.

[2 marks]

_____

_____

_____

_____

6

Turn over ▶

Do not write outside the box

1 4 A company network can be kept secure, and data protected when transferred electronically, by following simple and routine security protocols.

1 4 . 1 Explain how **MAC association** and the **DHCP server** can work together to better secure a network.

[2 marks]

1 4 . 2 A service set identifier (SSID) is used with wireless local area networks (WLAN), including home networks and public hotspots.

Explain why it is important to change SSID default settings.

[2 marks]

1 4 . 3 **Encryption** is the most effective way of securing data and asymmetric encryption is more secure than symmetric encryption.

Give **one** advantage of using **symmetric** encryption (rather than asymmetric encryption) and **one** security challenge inevitable when using **symmetric** encryption.

[2 marks]

6

Do not write outside the box

1 5 Banner grabbing and port scanning are two network monitoring tools.

For both network monitoring tools identify:

- the information it can provide
- how a hacker might exploit this tool
- what counter-measures you might apply.

[6 marks]

Banner grabbing _____

_____

_____

_____

_____

_____

Port scanning _____

_____

_____

_____

_____

_____

6

Do not write outside the box

1 6 As a network manager you have been asked to review the network security plan for new clients.

Explain how you would monitor a network system open to all (employees and visitors, with both deskbound access and remote access) ensuring security is maintained at all times.

[6 marks]

6

Do not write outside the box

Section B

1 7 **Network access control (NAC)** restricts the availability of network resources to endpoint devices and was once thought appropriate only for user environments that could be rigidly controlled.

BYOD (bring your own device) – the use of employee-owned mobile devices such as smartphones, tablets, and laptops – enables end users to make use of not just corporate-owned devices but personal ones to access workplace content and networks.

1 7 . 1 Give **two benefits** of allowing employees to BYOD and explain why network managers accommodate this risk.

[4 marks]

1 7 . 2 Discuss the **security challenges** in having a BYOD environment.

[8 marks]

Do not write outside the box

1 7 . 3 As Network Manager of a BYOD environment, explain how you would ensure **secure network access** for all BYOD users – not just permanent employees, but temporary staff, visitors, and contractors alike.

[8 marks]

Do not write outside the box

1 7 . 4 Given the risks of BYOD to data control, list **four** things that a BYOD policy might include.

[4 marks]

1 7 . 5 The UK Information Commissioner's Office (ICO) has published BYOD guidance **for employers** on how to comply with the UK Data Protection Act 1998.

Identify **two** specific requirements this guidance might include.

[2 marks]

Turn over for the next question

Do not write outside the box

1 7 . 6 Multi-factor authentication provides greater security by requiring more than one identifier.

Give **two** examples of possible access control combinations.

[4 marks]

30

END OF QUESTIONS

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

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

For confidentiality purposes, from the November 2015 examination series, acknowledgements of third party copyright material will be published in a separate booklet rather than including them on the examination paper or support materials. This booklet is published after each examination series and is available for free download from www.aqa.org.uk after the live examination series.

Permission to reproduce all copyright material has been applied for. In some cases, efforts to contact copyright-holders may have been unsuccessful and AQA will be happy to rectify any omissions of acknowledgements. If you have any queries please contact the Copyright Team, AQA, Stag Hill House, Guildford, GU2 7XJ.

Copyright © 2018 AQA and its licensors. All rights reserved.