CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

Unit 3 January 2019 series

Version 1

Contents

Introduction

Our examiners' reports are produced to offer constructive feedback on candidates' performance in the examinations. They provide useful guidance for future candidates. The reports will include a general commentary on candidates' performance, identify technical aspects examined in the questions and highlight good performance and where performance could be improved. The reports will also explain aspects which caused difficulty and why the difficulties arose, whether through a lack of knowledge, poor examination technique, or any other identifiable and explainable reason.

Where overall performance on a question/question part was considered good, with no particular areas to highlight, these questions have not been included in the report. A full copy of the question paper can be downloaded from OCR.

Unit 3 series overview

In general there was an increase in the level of technical language and an improvement in the understanding of the underlying principles of cyber security. There does however remain a significant number of candidates for whom identity theft and fraud appear to be their go to answers. Whilst Section B will always be more challenging as it is unseen, it is clear that many candidates are not overly familiar with the case study.

High marks require three elements: knowledge of the subject area, an understanding of the requirements of the keyword in the question and an application of the answer to the scenario. In many of the responses marked, one or more of these elements was missing.

Section A overview

Section A was based on the case study and associated tasks. It was based around a Kathmandu Coffee shop where one of its visitors was involved in a cyber security incident. The pre-release included several themes for research that formed the basis of the questions asked within the paper.

Question 1(a)

This section relates to the case study about a cyber security attack on a customer in Nepal.

1   Whilst on holiday in Kathmandu, Mr Thapa used a Wi-Fi access point in a coffee shop to connect his personal mobile phone to the internet to perform a number of tasks. Whilst connected his phone was hacked.

   (a)   The diagram below shows three types of attacker and three definitions.

   Draw a line to connect each type of attacker to its correct definition.

Type of attacker	Definition
hactivist	individual who often sends an email trying to get you to pay for goods or opportunities without there being any real end product
phisher	individual who tries to obtain financial or confidential information by sending an email that looks like it has come from a legitimate organisation
scammer	individual who uses computers to promote their own views on a particular issue

[3]

This was done very well by the majority of candidates. Those who answered it incorrectly confused Scammer and Phisher.

Question 1(b)

(b) Explain **one** reason why Mr Thapa would want to keep his phone secure.

....

....

....

....**[2]**

As an explanation, a superficial answer did not gain credit. Answers that referred to personal or sensitive information were not detailed enough and did not include the reason that an explanation demands.

Question 1(c)

(c) One type of attacker is a script kiddie. Complete the table below to identify the likely characteristics of a script kiddie.

Characteristic	Script kiddie
age	
location	
social group	

[3]

Many of the responses for age were marked correct and location was done reasonably well. Social group was not answered very well with many stating that they would not be a member of a group. A social group does not just have to be a physical society; it can be an online society as well. Whilst, as many candidates suggested, they would not have any friends at school, they did not consider the digital communities they might be a part of.

Question 1(d)

(d) Discuss the reasons why people, such as Mr. Thapa, can be targets of cyber security attacks in a coffee shop environment.

[7]

....

....

....

....

There were two ways this question could have been answered. Firstly, why a coffee shop was a good environment to use to target people in a cyber security attack and secondly, why Mr Thapa was a likely target of a cyber security attack.

Many of the responses focused on how the attack took place rather than why the target was selected. As a discussion, the depth of reason required to achieve high marks is considerable and many responses were merely lists in sentence form limited the amount of marks they could obtain.

Question 1(e)

(e) Identify and describe **one** method that could be used by attackers to access Mr Thapa's phone.

....

....

....

....**[3]**

This question was directly linked to the case study and needed to be a method that was likely to have occurred given the scenario. One mark was given for the identification of the method with a further 2 marks for a description of how this would have occurred. There was a wide variety of possible methods given though some of them would not have been possible or delivered the attack from the scenario.

Question 1(f)

Following the phone hack, personal information has been extracted from Mr Thapa's phone by the attacker.

(f) Using examples, describe **three different** ways Mr Thapa's life could be disrupted by cyber criminals using the information obtained from the phone hack.

1...

....

....

....

2...

....

....

....

3...

....

....

....

[6]

The use of information gained needed to clearly disrupt Mr Thapa's life. Identification of what could be obtained was not enough to gain the marks; the candidate needed to go on to show how a cyber criminal having and using this information has a detrimental effect on Mr Thapa.

Question 1(g)

(g) Describe **two different** access controls Mr Thapa could implement to secure his phone.

1...

....

....

....

2...

....

....

....

[4]

The key word in this question was access control. Many candidates gave methods that he could use but they were not access controls and so gained no marks.

Question 2(a)

The franchise that owns the coffee shop has employed a cyber security team to investigate the hack into Mr Thapa's phone.

2   (a)   Identify **three** pieces of information Mr Thapa needs to provide to the cyber security team in order for them to create a cyber security incident report. For **each** piece of information, state why it is needed by the cyber security team.

1..

....

Why needed ....

....

2..

....

Why needed ....

....

3..

....

Why needed ....

....

[6]

This question was answered very well with many candidates gaining high marks. Marks were lost where candidates expected Mr Thapa to give information that would be included in the report but would not have come from him – motivation or intention of the criminal, method used to hack the phone and so on.

It is important that the candidate selects the appropriate response that fits the scenario from the possible answers. Many incorrect answers were headings on the cyber security report and correct for a different question.

Question 2(b)

(b) Mr Thapa has been asked to cooperate with the cyber security team during its investigation.

Explain why it is important to Mr Thapa that each member of the cyber security team has a different role.

....

....

....

....**[2]**

There were three aspects to this question. Firstly an explanation, which requires 'an account of the purposes or reasons'. Secondly why there is a division of roles within a security team and thirdly and most importantly, why this division of roles is important to Mr Thapa. The third point was generally the element that was missed by many candidates. This was the key to the question. Many responses gave reasons why there were different people but not why this was important to Mr Thapa or how it related to him.

Question 2(c)

(c) Explain **two** ways that the coffee shop could use the review of the incident created by the cyber security team.

1...

....

....

....

2...

....

....

....

[4]

The use of the review comes after the report has been completed. It is the action that the coffee shop can take based on what the review has concluded happened. Many of the responses were generally in the right area but lacked the detail required at this level. This question followed on from the scenario and how Mr Thapa was hacked and therefore how the coffee should can prevent it. A technical understanding is required the befits a programme of study about cyber security.

Section B overview

Section B assessed knowledge from across the specification and was not linked to the scenario.

Question 3

You do not need the case study to answer these questions.

3   Describe, using an example, how cyber security aims to protect the confidentiality, integrity and availability of data.

Confidentiality ....

....

....

....

Integrity ....

....

....

....

Availability ....

....

....

....

[6]

The CIA triad is the cornerstone of cyber security. The 'how' in the question requires a practical solution that can be implemented. Many candidates were unclear on the differences between the three and any descriptions that reuse the keyword without amplification cannot be given marks.

Question 4(a)*

4   (a)* Justify the effectiveness of using network intrusion detection systems (NIDS) to protect
          the information stored on a server.

                                                                                              [10]

          ....

          ....

          ....

          ....

There were several elements to this question. A justification is 'a reasoned case for actions or decisions made' – in other words, relating to the question, why should a NIDS be used. This requires positive reasons only. It was not an evaluation or discussion but a justification.

The second key element was the focus on the effectiveness of the NIDS. Many candidates chose to list its features rather than how those features were effective in protecting the network.

This question showed a lack of understanding of NIDS as many of the responses given could have been applied to any IDS and lacked a technical knowledge and understanding of this key element of network security.

Question 4(b)

   (b) Identify **one other** type of intrusion detection system that could be used.

          ....**[1]**

Although generally answered very well there were a number of candidates who gave NIDS and many who gave an abbreviation but then wrote the terms out in full – incorrectly.

Question 5

5 A company should regularly undertake cyber security risk management.

Explain why it is not possible to remove all risk.

....

....

....

....

....

....**[3]**

This was very well answered with many candidates aware of risk and how it could not be eliminated. It was good to see candidates giving a range of reasons including from insiders, the human element, the competition between hackers and defenders and the impossibility of eliminating bugs.

Very few however obtained full marks as their answers were descriptive rather than an explanation.

Copyright

Any reference to existing companies or organisations is entirely coincidental and is not intended as a depiction of those companies or organisations.

Supporting you

For further details of this qualification please visit the subject webpage.

Review of results

If any of your students' results are not as expected, you may wish to consider one of our review of results services. For full information about the options available visit the OCR website. If university places are at stake you may wish to consider priority service 2 reviews of marking which have an earlier deadline to ensure your reviews are processed in time for university applications.

CPD Hub
Your route to OCR's teacher training

Attend one of our popular CPD courses to hear exam feedback directly from a senior assessor or drop in to an online Q&A session.

https://www.cpdhub.ocr.org.uk

We'd like to know your view on the resources we produce. By clicking on the 'Like' or 'Dislike' button you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

Whether you already offer OCR qualifications, are new to OCR, or are considering switching from your current provider/awarding organisation, you can request more information by completing the Expression of Interest form which can be found here: www.ocr.org.uk/expression-of-interest

OCR Resources: *the small print*
OCR's resources are provided to support the delivery of OCR qualifications, but in no way constitute an endorsed teaching method that is required by OCR. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources. We update our resources on a regular basis, so please check the OCR website to ensure you have the most up to date version.

This resource may be freely copied and distributed, as long as the OCR logo and this small print remain intact and OCR is acknowledged as the originator of this work.

Our documents are updated over time. Whilst every effort is made to check all documents, there may be contradictions between published support and the specification, therefore please use the information on the latest specification at all times. Where changes are made to specifications these will be indicated within the document, there will be a new version number indicated, and a summary of the changes. If you do notice a discrepancy between the specification and a resource please contact us at: resources.feedback@ocr.org.uk.

OCR acknowledges the use of the following content:
Square down and Square up: alexwhite/Shutterstock.com

Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk

Looking for a resource?

There is now a quick and easy search tool to help find **free** resources for your qualification:

www.ocr.org.uk/i-want-to/find-resources/

www.ocr.org.uk

OCR Customer Support Centre

Vocational qualifications
Telephone 02476 851509
Facsimile   02476 851633
Email vocational.qualifications@ocr.org.uk

OCR is part of Cambridge Assessment, a department of the University of Cambridge. *For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored.*