OCR
Oxford Cambridge and RSA

Cambridge **TECHNICALS LEVEL 3**

Cambridge TECHNICALS

IT

Feedback on the June 2018 exam paper (including selected exemplar candidate answers and commentary)

Unit 3 – Cyber security

Version 1

ocr.org.uk/ict

CONTENTS

INTRODUCTION

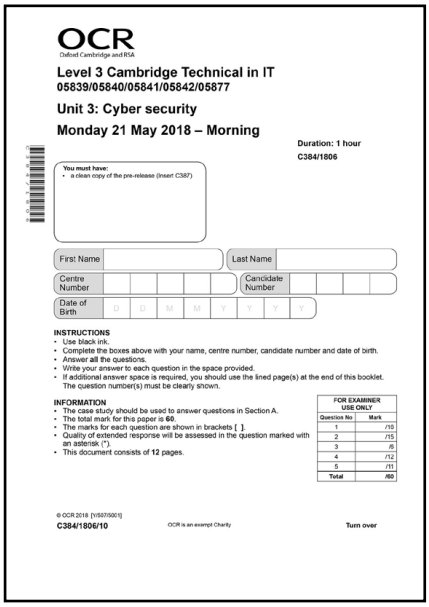
This resource brings together the questions from the June 2018 examined unit (Unit 3), the marking guidance, the examiners comments and the exemplar answers into one place for easy reference.

We have also included exemplar candidate answers with commentary for Questions 2(c), 4(b) and 5(b).

The marking guidance and the examiner's comments are taken from the Report to Centre for this question paper.

The Question Paper, Mark Scheme and the Report to Centre are available from:

https://interchange.ocr.org.uk/Modules/PastPapers/Pages/PastPapers.aspx?menuindex=97&menuid=250



OCR
Oxford Cambridge and RSA

Level 3 Cambridge Technical in IT
05839/05840/05841/05842/05877

Unit 3: Cyber security

Monday 21 May 2018 – Morning

Duration: 1 hour
C384/1806

You must have:
- a clean copy of the pre-release (insert C387)

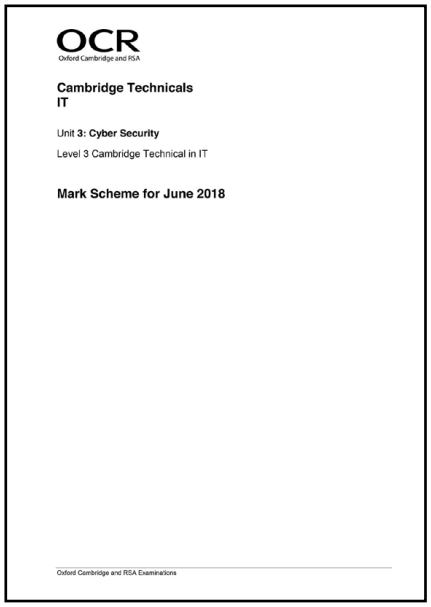
First Name | Last Name
Centre Number | Candidate Number
Date of Birth (D D M M Y Y Y Y)

INSTRUCTIONS
- Use black ink.
- Complete the boxes above with your name, centre number, candidate number and date of birth.
- Answer **all** the questions.
- Write your answer to each question in the space provided.
- If additional answer space is required, you should use the lined page(s) at the end of this booklet. The question number(s) must be clearly shown.

INFORMATION
- The case study should be used to answer questions in Section A.
- The total mark for this paper is **60**.
- The marks for each question are shown in brackets [ ].
- Quality of extended response will be assessed in the question marked with an asterisk (*).
- This document consists of **12** pages.

FOR EXAMINER USE ONLY	
Question No	Mark
1	/15
2	/15
3	/5
4	/12
5	/11
Total	**/60**

C384/1806/10 OCR is an exempt Charity **Turn over**



OCR
Oxford Cambridge and RSA

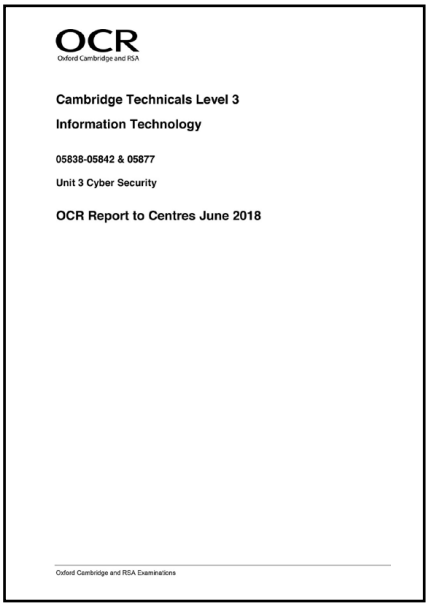
Cambridge Technicals
IT

Unit **3: Cyber Security**

Level 3 Cambridge Technical in IT

Mark Scheme for June 2018

Oxford Cambridge and RSA Examinations



OCR
Oxford Cambridge and RSA

Cambridge Technicals Level 3
Information Technology

05838-05842 & 05877

Unit 3 Cyber Security

OCR Report to Centres June 2018

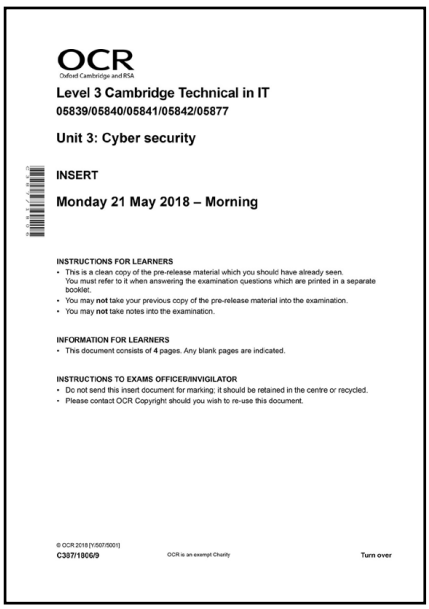
Oxford Cambridge and RSA Examinations

PRE-RELEASE MATERIAL

The question paper is based on a pre-release research brief which is issued to centres 6-8 weeks before the examination.

Learners should refer to this pre-release material to answer questions in the question paper.

The pre-release Research Brief can be found on Interchange.



OCR
Oxford Cambridge and RSA

Level 3 Cambridge Technical in IT
05839/05840/05841/05842/05877

Unit 3: Cyber security

INSERT

Monday 21 May 2018 – Morning

INSTRUCTIONS FOR LEARNERS
- This is a clean copy of the pre-release material which you should have already seen. You must refer to it when answering the examination questions which are printed in a separate booklet.
- You may **not** take your previous copy of the pre-release material into the examination.
- You may **not** take notes into the examination.

INFORMATION FOR LEARNERS
- This document consists of **4** pages. Any blank pages are indicated.

INSTRUCTIONS TO EXAMS OFFICER/INVIGILATOR
- Do not send this insert document for marking; it should be retained in the centre or recycled.
- Please contact OCR Copyright should you wish to re-use this document.

C387/1806/9 OCR is an exempt Charity **Turn over**

Pre-release material

Digital Personal Assistant

Background

A digital personal assistant is a device that responds to vocal commands. It is activated by a keyword and will then run a command based on the vocal input from the user. Commands can include, amongst other things:

- web searches;
- playing music;
- creating/amending shopping lists;
- creating/amending to do lists;
- purchasing items from the web.

Mr. Daka

Mr. Daka lives at home with his wife and two teenage children. He is interested in new technologies and their ability to automate everyday tasks.

Mr. Daka has purchased a digital personal assistant for his home. He has integrated the device into his home automation system. This has included:

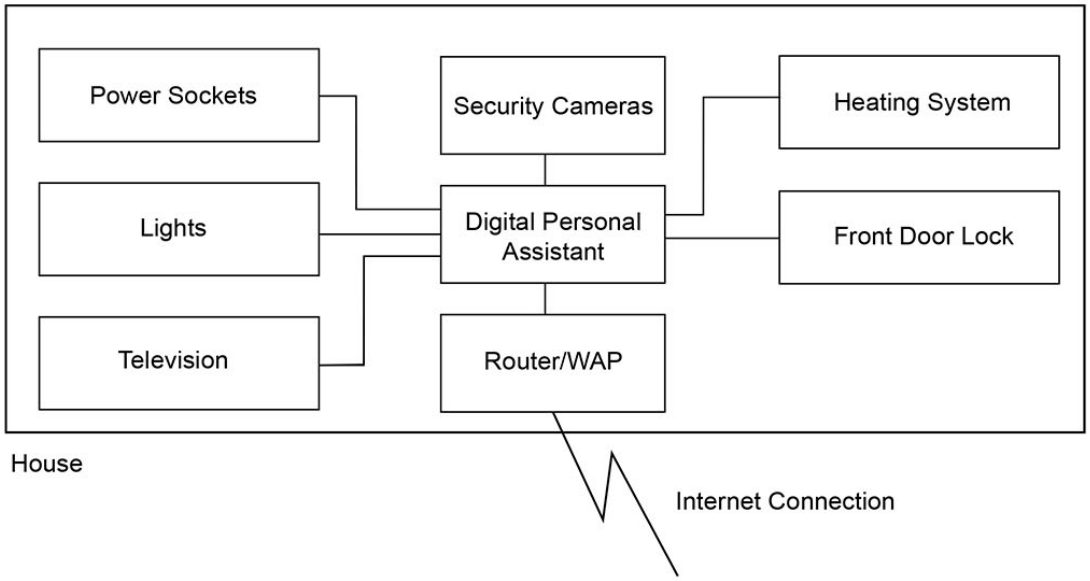
- security cameras;
- heating system;
- home entertainment systems;
- lights and power sockets;
- home locking mechanisms.

Set Up

Mr. Daka has a single internet connection into the house which plugs into a hybrid router, combining routing, switching and a wireless access point (WAP) into a single device, given to him by his internet service provider.

Mr. Daka has set the system up so that he can control his devices and change settings through a variety of apps on his smartphone. This allows him to perform tasks such as turning lights on and off, adjusting heating, opening the front door and viewing security cameras when he is away from his home.

Diagram of Digital Personal Assistant and Home Automation Integration



To prepare for the examination, you should research the following themes:

- information needed by an attacker to gain access to the digital personal assistant and connected devices;
- different devices that can be connected in a home automation system and the implications for each type of device of being attacked;
- methods that could be used to exploit and mitigate against vulnerabilities in the different connected devices;
- different types of attackers who might want to access the digital personal assistant and their motivations.

GENERAL EXAMINER COMMENTS ON THE PAPER

The continued improvement session on session was fully evident in this paper. Many candidates were able to cope well with the rigors of the paper and gave some really good answers.

However, there also remains a significant number of candidates who appear to be lacking any depth of understanding and knowledge. Whilst the unseen section of the paper is always going to be more challenging, section A can be prepared for and it was disappointing that many candidates seemed ill-prepared for this section of the paper.

Resources which might help address the examiner comments:

From the link below, you'll find 'The OCR guide to examinations' (along with many other skills guides)
http://www.ocr.org.uk/i-want-to/skills-guides/

Command verbs definitions
http://www.ocr.org.uk/Images/273311-command-verbs-definitions.pdf

Questions 1(a), (b) and (c)

Answer **all** the questions.

Section A

This section relates to the case study on Digital Personal Assistant.

1 The digital personal assistant has access to a large amount of personal information about Mr. Daka.

(a) Explain **two** reasons why it is important for Mr. Daka to protect his personal information.

1. **Possible reasons why it is important for Mr. Daka to protect his personal information include:**
   - Can lead to identify theft/fraud (1) can get enough information to persuade others they are him/if (example) date and place of birth are known/implication of identity theft (1).
   - Maintain his privacy (1) does not want all information about him revealed to public (1).
2. - Protect his finances (1) could withdraw money from his account or equivalent (1).
   - Can lead to blackmail (1) if personal information could be exploited (1).
   - To prevent unauthorised access (by a third party)/hacking (1) so they do not misuse personal information(1).
   - Any other valid suggestion.

[4]

Mr. Daka is concerned about how secure the digital personal assistant is from attackers.

(b) Identify **two** pieces of information that could be obtained from attacking Mr. Daka's digital personal assistant.

1. **Possible pieces of information include:**
2. - Date of birth (1)
   - User name (1)
   - Online password to website (1)
   - Address (1)
   - When present/not present in the house (1)
   - Current status of any device controlled by the DPA (1)
   - Financial information (or examples thereof) (1)
   - Questions/searches (NOT activities) that have been asked (1)
   - Any other valid suggestion.

[2]

(c) Identify **two** pieces of information that would be needed to launch a system attack on Mr. Daka's digital personal assistant.

1. **Possible pieces of information include:**
2. - IP/MAC address of router/equivalent device (1)
   - Password/passcode (1)
   - Username (1)
   - Version of software (1)
   - Any other valid suggestion.

[2]

Mark Scheme Guidance

Question 1(a):

Up to two marks for each of two explanations.

One mark is for identifying a reason. Award ANY reasonable reason that shows why personal information should be protected (**this is an implication of the information being stolen not the initial protection**). Second mark is for explaining why/how it is a reason (candidate can identify the personal details that are lost as part of the "how").

Answer may be an implication of data theft, or deal with the theft in the first place (bullet point 5).

Numbers on lines are for guidance only. Candidate may answer wholly within section 1, for example.

Mark first two explanations ONLY.

DO NOT accept non-personal information – such as password or address.

Question 1(b):

Should be realistic and available from a personal digital assistant. However, information held on the DPA can includes shopping lists, to do lists etc.

For password, allow specific examples.

DO NOT allow:

- Medical records
- Personal information
- Current location.

Question 1(c):

For two marks:

Allow information relating to Mr. Daka, the network, or the device.

Allow any reference to password/passcode.

Examiner comments

Question 1(a) – The vast majority of candidates were able to explain at least one reason why personal information should be protected, with most being able to explain two reasons. In a few cases, candidates knew why personal information should be protected, but gave weak expansions, such as "because he does not want someone else to know things about him". Answers such as this, which are extremely general, as not sufficient for this level of examination.

Question 1(b) – There are many items of information that may be garnered by accessing a digital personal assistant. As a consequence, the vast majority of candidates gave two good answers for this question. In a very small number of instances, candidates did not seem to fully appreciate what a digital personal assistant is and so gave answers that were not acceptable within the breadth of answers accepted.

Question 1(c) – Whilst the breadth of possible answers for this question did not match the breadth of the previous, examiners were aware that many possible answers existed and awarded accordingly. However, answers such as "his address" were not accepted.

Questions 1(d) and (e)

(d) Describe **two** different methods an attacker could use to get personal information directly from Mr. Daka.

1 ....

Possible methods an attacker could use to get personal information directly from Mr. Daka include:

- Social engineering (1) pretending to be from bank/software company (1)
- Pharming (1) user directed to fake website (1)
- Phishing (1) email claiming to be from an authority/bank etc/demand for personal information (1)
- Scamming (1) use of fraudulent means (or example)/encourages installation of malware (1)

2 ....

- Spyware (1) which records key strokes (1)
- Gain access to security cameras (1) to read bank card details (1)
- Any other valid suggestion.

.....

.....

[4]

Mr. Daka is concerned that an attacker accessing the digital personal assistant could do more than just find information.

(e) Explain **two** ways that a cyber attack on the digital personal assistant could result in a physical vulnerability to his property.

1 ....

Possible ways a cyber-attack on the digital personal assistant could result in a physical vulnerability to his property include:

- Turning the heating off (1) can lead to frozen pipes (1)
- Door can be opened remotely (1) allowing access to property (1)
- Alarm systems can be switched off (1) so if a break in occurs they will not go off (1)
- Cameras/microphone can be accessed (1) to see if Mr. Daka is at home (1)
- Create a power surge (1) so that fuse board/router trips (1)

2 ....

- Any other valid suggestion.

.....

.....

.....

[4]

Mark Scheme Guidance

Question 1(d):

Up to two marks for each of two descriptions.

One mark for method (accept NOUN or VERB). Method may be passive OR active.

Another mark for description of that method. NB does not need to state the type of personal information accessed/got.

Attack MUST be a cyberattack. DO NOT accept attacks which are clearly physical.

DO NOT accept "hacking" e.g.:

"Hacking by cracking a wifi password" – 1 mark for underlined portion of answer only.

Question 1(e):

Up to two marks for each of two explanations.

Needs to involve something physical occurring at/to the property, not just data. Expansion must explain the physical vulnerability. For example – change door pass code (1) so that the house can be burgled (1).

Do not award expansions which deal with after the event consequences (such as delete camera recording so that evidence of robbery deleted).

Examiner comments

Question 1(d) – This question required candidates to describe two types of cyberattack that could be carried out and which would obtain personal data from Mr Daka. This description had to be of the method employed, so the first mark for each description was awarded for the identification of the method. The second mark was the expansion to give a description.

Many candidates gave good answers here, with Phishing, Pharming and Social Engineering all appearing regularly. However, candidates who simply stated "hacking" were not awarded a mark, and neither were candidates who suggested methods, such as physical assault.

Question 1(e) – The vast majority of candidates realised that the digital personal assistant had direct control and access to physical controls, such as doors and heating and therefore any third party control was a potential risk. Answers tended to concentrate on the physical risk caused by opening doors/disabling locks and these answers were generally well explained. However, the second answer, usually focussing on access to heating, was not well explained, with candidates simply stating that heating could be turned up.

Questions 2(a) and (b)

2 There are many different types of attackers who could gain access to the digital personal assistant. One type is a vulnerability broker.

(a) Describe what is meant by a vulnerability broker.

Possible responses include:
- Individual who sells information (1st)
- To a third party/example (1)
- Information includes flaws in a device/how to access device (1)
- Information on how to hack into the device (1)
- Any other valid suggestion (1).

.....
.....
.....
.....
[2]

(b) Describe **two** reasons why Mr. Daka should be concerned by a vulnerability broker having information about the digital personal assistant.

1 ....
.....
.....
2 ....

Possible reasons why Mr. Daka should be concerned by a vulnerability broker having information about the digital personal assistant include:
- The broker needs (issues to sell) (1) (if he has found them) means there is a flaw in the system (1) multiple individuals can buy the flaw and gain access (1)
- Company has not fully tested the product (1) might be other issues with the technology (1)
- Broker can sell/pass on the information (1) one implication (1)
- Any other valid suggestion.

.....
.....
.....
[4]

Mark Scheme Guidance

Question 2(a):

Up to two marks for description.

Answer must clearly deal with the broker selling information that is found. This is NOT the same as being employed to identify issues.

Expansion must be more than simply stating "about vulnerabilities". Must be an example of.

Question 2(b):

Up to two marks for each of two descriptions.

Answers must be about the fact that the vulnerability broker has obtained the data (such as Why? How?).

Vulnerability broker who uses the data themselves is not a VB by definition.

Examiner comments

Question 2 – This question focussed on the types of attackers who could target a digital personal assistant and their motivations.

Question 2(a) – For question 2 (a), the key point about a vulnerability broker was that they sell, or attempt to sell, data. Where candidates simply stated that a vulnerability broker stole information, or looked for easy access to systems, this was not sufficient, as these definitions were not considered specific enough.

Question 2(b) – This question proved to be quite a challenge to many candidates. One acceptable answer was that the broker would have data about Mr Daka, but all others were to do with any concern Mr Daka should have in general terms.

Most candidates appreciated that the broker could sell information to a third party, with a negative outcome, but were then unable to give any further impacts. This would suggest that many candidates had prepared by considering impact on Mr Daka, but had not prepared by considering wider impacts.

Questions 2(c) and (d)

One motivation for attackers is income generation.

(c) Identify and describe **two other** motivations an attacker might have for attacking Mr. Daka's digital personal assistant.

1 .....

.....

.....

.....

.....

.....

2 .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

[6]

Possible motivations include:

- To gain personal information (1st) that can be used in a crime (1) such as identity theft (1).
- Public Good (1st) raising awareness of a vulnerability so company can patch it (1) reducing opportunities for hacking (1).
- Thrill (1st) finding out if the device can be hacked (1) beating fellow hackers to find the vulnerability (1).
- Blackmail (1st) use of information (1) to make Mr Daka do something he would rather not do (1).
- Personal vengeance (1st) negative impact on Mr Daka (1) to redress some previous hurt (1).
- Havoc and mayhem (1st) to cause disruption (1) for a personal thrill (1).
- Publicity (1st) name becomes known (1) for deep joy (1).
- Any other valid suggestion.

The brand of digital personal assistant used by Mr. Daka has recently been targeted by organised crime.

(d) Explain why individuals involved in organised crime would want to target digital personal assistants.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

[3]

Possible responses include:

- If all devices have the same vulnerability (1) allows access to many devices with same hack (1) do not have to spend time researching/running each hack (1).
- Large number of homes/devices (1) with the same vulnerability (1) makes it easier to blackmail/extort money from developer/earn money (1).
- Any other valid suggestion.

Mark Scheme Guidance

Question 2(c):

In each of two cases:

Need to identify motivation before description marks can be awarded.

Do not allow income generation of any type as an example.

OR expansion (fraud is acceptable, as can lead to personal gain).

Question 2(d):

Up to three marks for explanation.

Answers must deal with an **attack on the brand**, rather than an attack on an individual DPA.

Examiner comments

Question 2(c) – A significant minority of candidates missed the advice that they should give motivations other than financial. Where candidates gave answers that could lead to financial gain, but could equally lead to non-financial gain (such as identity theft) and did not specifically state that the outcome would be a financial gain, marks were awarded.

Where candidates did take note of the direction, many marks were awarded. This area of the syllabus would appear to be a strength, with many candidates scoring very well indeed.

Question 2(d) – As with question 2 (b), candidates failed to take note of the context of this question and gave general answers about individual attacks on individual digital personal assistants. However, the question was actually about an attack on the brand of the digital personal assistant and therefore was looking for an understanding of the interaction between a digital threat and business. Very few candidates scored any marks for this question.

Exemplar candidate work

Question 2(c) – Low level answer

One motivation for attackers is income generation.

(c) Identify and describe **two other** motivations an attacker might have for attacking Mr. Daka's digital personal assistant.

1 Some attackers Purely hack others Just to see if it is possible, they usually don't have a malicious intent to modify or steal information. It's purely for self reasoning.

2 malicious intent is another because some people may want to modify his information or find out information such as passwords etc.

[6]

Commentary

This candidate has been awarded one mark for the first point made in the first answer. Some attackers do hack to see if it is possible, but it would be wrong to say this is not malicious.

The second answer of "malicious intent" is too vague in a course that specifically focuses on the possible motivations of hackers. As the overall mark was awarded for first identifying a motivation, no further marks were available.

In order to improve this answer, the candidate should be clearer about what they mean by malicious intent. There are numerous examples in the syllabus.

Question 3

3 The developer of the digital personal assistant can only protect the device from security vulnerabilities. The network also needs to be secured. Password strength of the router is one area that is dependent on the network and not the digital personal assistant.

(a) Describe **two other** areas that should be examined for security vulnerabilities that are dependent on Mr. Daka's network and **not** the digital personal assistant.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

[4]

Possible areas that should be examined for security vulnerabilities that are dependent on Mr. Daka's network and not the digital assistant include:

- Access controls (1) which accounts have access to which parts of the system/ level of access of different accounts (1).
- Wifi security (1) encryption enabled/ssid hidden (1).
- Default settings (1) have they been changed (1).
- Open ports (1) which ports on the router are open/available (1)
- Firewall (1) to check that it is checking all/any traffic (1)
- Any other valid suggestion.

Fuzzing is one method that could be used to test new systems for security vulnerabilities.

(b) Describe how fuzzing could be used to test Mr. Daka's digital personal assistant.

.....

.....

.....

[2]

Possible responses include:

- Overload the system with data (1st)
- See how it responds/make sure it does not crash/check whether does crash (1)
- Any other valid suggestion.

Mark Scheme Guidance

Question 3(a):

Up to two marks for each of two descriptions.

Question 3(b):

Up to two marks for description.

Examiner comments

Question 3 explored candidates' understanding of wider areas of vulnerability.

Questions 3(a) and (b) – As a cohort, candidates did not seem confident with either of these areas. In a few cases, candidates showed good technical understanding of network vulnerabilities and earned good marks. However, the majority of candidates gave general answers that showed little technical understanding. Similarly, with question 3 (b), candidates knew that fuzzing was an attack, but few knew the fundamental point that this form of attack overloads the system with data.

Question 4

Section B

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

4 Two methods of security management for computers and networks are network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS).

(a) Describe the difference between NIDS and HIDS.

Possible responses include:
- HIDS – installed on every network computer (1)
- NIDS – only installed at specific points (1)
- HIDS – all devices with two way access to external environment (1)
- NIDS – installed on devices that sit between network and external environment (1)
- HIDS – only examines traffic directed at host/single computer it is protecting (1)
- NIDS – examines all traffic (1)
- Any other valid suggestion.

[2]

(b)* Evaluate the use of intrusion detection systems (IDS) as a method for protecting a network.

[10]

Indicative content:
- There are different types of IDS which can provide different functions, no single IDS will provide all functions meaning that either multiple IDS need to be run using resources or there may be gaps in the functionality.
- Alarms are raised in real time but this requires a network operator to be available and monitoring in order to react.
- Hacker may use signatures (for example) that are matched within the rule base and so will not raise the alarm.
- Signatures cannot be detected if they are not in the rule base only making them useful for attacks that have happened elsewhere.
- False positives can be flagged wasting investigation time.
- IDS continue to improve over time as signatures continually added to the IDS model.
- IDS look for known weaknesses, these can be avoided by hackers.
- Any other valid suggestion.

Mark Scheme Guidance

Question 4(a):

Up to two marks for description.

Can award one mark for a statement about either system.

For full marks, must be a comparison, not two individual unrelated statements

Question 4(b):

Mark Band 3 (7-10 marks)

The learner has explained the advantages and disadvantages of using an IDS as a method for protecting a network. Both sides of the argument are considered with some attempt to prioritise the information that is given.

Subject specific terminology and knowledge will be clearly used to support and inform the explanations.

There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.

Mark Band 2 (4-6 marks)

The learner has described how an IDS might be used to protect a network. There is some consideration of advantages and/or disadvantages.

At the bottom end of this mark band, the learner may give a generic description of how an IDS works.

There is a line of reasoning presented with some structure. The information presented is for the most part relevant and supported by some evidence.

Mark Band 1 (1-3 marks)

The learner has identified generic points in relation to an IDS. Subject specific terminology may be limited or missing.

The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.

0 marks = Nothing worthy of credit.

Examiner comments

Section B assessed knowledge from across the syllabus and is not linked to the scenario.

Question 4 – This question focussed on methods of security management.

Question 4(a) – Many candidates scored well here, with most candidates focussing on the area being monitored.

Question 4(b) – This question assessed understanding, as well as candidates' ability to express themselves eloquently.

Candidates were asked to evaluate the use of an IDS system to protect a network. Where this was answered well, candidates gave full answers that discussed the positive aspects of an IDS as well as the negative aspects. These answers were balanced, well expressed and evaluative of the overall impact.

However, other candidates made a few simple points about IDS and did evaluate their usefulness, whilst others made a few points and went onto discuss other methods of protection. Whilst a discussion of other methods of protection may be seen as a supporting point to a general discussion of IDS, this is most definitely not a sound answer when used on its own.

Exemplar candidate work

Question 4(b) – Medium level answer

(b)* Evaluate the use of intrusion detection systems (IDS) as a method for protecting a network.

[10]

An intrusion detection system is a software used monitor trafic on a network. It has got its positives and negives. An intrusion detection system has many different ways of protecting a network. They have got NIDS, which can be used for the entire network and what is going in and out of the network by intercepting small data packets. However most importantly, AIDS is more significant in which devices of the network are continued. This is good because surveillance has been placed which on the other hand, some employees of an organisation may disagree with as they may find it unethical. Ultimately, it would be good as if any of the employees in an organisation goes on any illegal, unusual or unathorise thing, this will immediately be alerted to the administrator. The negative are that unfortunately, unlike an IPS, and IDS will not have the ability to block any attacks or security breaches. For example if a entity by accident downloaded a software full of viruses the IDS will only alert this danger to the IT administrators it will not automatically avoid and block the danger.

Commentary

This is a clear example of a candidate who has hit the middle band by describing the focus of the question, and therefore only partially addressing the actual reason behind the question.

The work here describing an Intrusion Detection System (IDS) is not particularly detailed. It does include some discussion of how an IDS is important, which goes some way towards the evaluation that is required. However, as the description of an IDS is not as clear or as detailed as it could be, a mark from the middle of the mark band, rather than the top, is more appropriate.

Had the candidate been more focused in their answer and looked at both positives and negatives of the method, they would have moved into MB3.

Question 5

5 A travel agency has had its network attacked and information on its customers has been accessed. A private security firm, SafeWithUs has been hired to investigate the attack. SafeWithUs has completed a cyber security incident report as part of the investigation.

One of the sections completed in the cyber security incident report is the capability of the attackers. One way the capability of the attacker could be determined is by the techniques that they used.

(a) Describe **two other** ways SafeWithUs could determine the capability of the attackers.

1 .....

.....

.....

.....

2 .....

.....

Possible ways SafeWithUs could determine the capability of the attackers include:

- Time they spent in the system (1st) this will determine if they knew what they were doing/structure of the system (1).
- Examine any logs for where accessed/what could not access (1st) to identify the levels of security that they could not beat (1).
- What trail was left behind (1st) to identify effectiveness/efficiency (1).
- Consider security used on the network (1st) to identify/gauge the level of security overcome (1).
- Any other valid suggestion.

[4]

Another section of the cyber security incident report deals with the techniques used by the attackers.

(b) Discuss why SafeWithUs needs to understand the techniques used by the attackers.

[7]

Indicative content:
Possible reasons why SafeWithUs needs to understand the techniques used by the attackers include:

- Profiling the attacker so that this individual/type of attacker can be protected against.
- To know how the attacker got in so that the vulnerability can be repaired and not exploited again.
- To know which part of the system were accessed by the attacker which will help them identify which data was accessed/compromised so customers/authorities can be notified.
- To know if it is the result of a script kiddie/vulnerability broker or if it is a new hack and they need to inform the hardware manufacturer.
- To determine where responsibility lies within the company and if any law has been broken, such as the DPA.
- Any other valid suggestion.

Mark Scheme Guidance

Question 5(a):

Up to two marks for each of two descriptions.

Do not allow techniques used/type of hacking.

This is not about the level of capability but how to find it out.

DO NOT accept location/country of origin.

Question 5(b):

Mark Band 3 (5-7 marks)

The learner has explained reasons why SafeWithUs needs to understand the techniques used by the attackers.

Mark Band 2 (3-4 marks)

The learner has described how the techniques used by attackers may inform the decisions taken by SafeWithUs around cyber security.

Mark Band 1 (1-2 marks)

The learner identifies generic points in relation to why knowledge of techniques used by attackers are important.

0 marks = Nothing worthy of credit.

Examiner comments

Question 5(a) – As with other questions in this paper, the main question directly excluded possible answers that candidates may give. Despite this, many candidates gave answers that were simply based on the method used and so could not be considered.

Where candidates did give other answers, many correctly identified that time spent in the system was a key indicator of the skill of the attackers, as well as the areas of the network to which the attacker was able to gain access. However, other candidates wrongly considered that the nature of the data stolen, or the impact of its theft, were important. Neither answer was acceptable.

Question 5(b) – This was well answered by many candidates, who were fully aware that a great deal could be learnt by investigating the techniques used by attackers, and that this information could be used by the investigators themselves and others.

Exemplar candidate work

Question 5(b) – High level answer

Another section of the cyber security incident report deals with the techniques used by the attackers.

(b) Discuss why SafeWithUs needs to understand the techniques used by the attackers.

[7]

One reason why safewithus needs to understand the technique is that they would be able to prevent such attacks from happening again, as they would know how this attack was done, so they would train staff in to ensure what to look for.

Another reason why Safe with us needs to understand the techniques is because they could relate it to previous attacks and is if ~~they~~ there is any repetiveness, and This is benefical as they would be able to tell if it is same person/ organisation committing the crime.

Futhermore, by understanding the techiques used, this would allows the company to do Patch updates on it networks, improve ~~they~~ Physical, hardware and software that is used to protect the information and ~~of~~ data.

Commentary

There is a clear flow to the individual paragraphs in this work. The first paragraph is very well written, with clear use of a point and expansion technique to explain why techniques need to be understood.

The second paragraph feels slightly rushed as it is not as well explained as the opening paragraph.

The final paragraph is a **description** of an advantage, rather than an **explanation** of why it is an advantage. Had the candidate explained why this would be an advantage, overall, this would have been a full mark answer. As it currently stands, this is still a top band answer.

The small print

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

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/

ocr.org.uk/it

OCR Customer Contact 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.*

Cambridge Assessment

LLOYD'S REGISTER · LRQA
ISO 9001
UKAS MANAGEMENT SYSTEMS
001