Level 3 Technical Level

IT: NETWORKING

Unit 6 Network security management
A/507/6495
Report on the Examination

TVQ01011
June 2018

Version: 1.0

Further copies of this Report are available from aqa.org.uk

One of the most challenging questions on this particular paper seems to have been Q15, with a few students making no attempt at this 6-mark question. This question related to a Security Service Level Agreement (SSLA) and criterion appropriate for measuring performance. It is accepted that sourcing locally available relevant information is likely to be met with difficulties given commercial sensitivities. It is also accepted that students are likely to find content more readily accessible — and find themselves more able to apply its relevance — following placement rather than by internet research alone.

Another challenging question was Q17. Again, a few students made no attempt. This question related to Continuous Network Security Monitoring (CNSM) and demanded an understanding and explanation of both front end and back end security. Overall, student responses to this 6-mark question were poor with students seeming not to have an adequate grasp of the fundamental content required.

One question, Q9, required students to suggest two disciplinary actions likely to be found within a Computer Acceptable Use Policy. It was clear from student responses that the question reference to 'disciplinary' was not always well understood, resulting in some inappropriate responses.

There were some recurrent themes, familiar from the previous paper, with, for example, Q5, Q10, and Q11 requiring an understanding of security standards and protocols; Q3, Q6, Q8, and Q13, and indeed Q20 (the most challenging question of this paper) all requiring an understanding system vulnerabilities, their testing, and amelioration.

Given that this is only the second live paper, much content was new: Q12.2 (risk assessments) and Q16 (packet sniffer) are both examples.

Q13 required an explanation of the role of the ethical hacker and was intended to allow students to demonstrate further their understanding of content and concepts tested in the single-mark Q3 multiple choice question, and in the two-mark Q8.

Responses were overall disappointing, for example:

- There was very little reference to replication of the likely actions of a malicious hacker so as to anticipate and better defend the likely actions of a malicious hacker.
- There was little reference to the ethical hacker acting in the best interests of the company and in a lawful and legitimate manner.
- It was rare for reference to be made to, or for there to be any comparison of, an ethical 'white hat' attack versus a malicious 'black hat' attack.

All three key features of an ethical hacker had been anticipated by the markscheme

The first five questions on this paper were single mark multiple choice questions and all were answered well.

There were a number of 2-mark questions (Q6, Q7, Q8, Q9, Q10.2, Q14.1).

- Q6, Q7, and Q14.1 were answered well, with most students achieving both marks for their Q7 and Q14.1 responses.
-
- Q9 was answered less well by some students (see above).

- the performance on Q10.2 tended to reverse what had happened on Q9.

- students made reference to WPA being more secure and / or making use of a longer password and this was deemed sufficient for a mark.

Of this paper's 3-mark questions, reference has already been made above to Q13; other 3-mark questions being Q11, Q12.1, and Q12.2:

- Q11 anticipated student responses would relate to hardware-based authentication (for example, tokens) or software-generated security (for example, one-time-passcodes / OTP authentication, encrypted signatures, or verification codes); the more successful student responses actually made reference to biometric security made possible due to developments within, for example, Apple's i-phone.

- Q12.1 demanded an understanding of a necessarily significant and extensive Network Security Plan that seemed unfamiliar to many students. Indeed, few students detailed sufficiently their understanding of how best to store or process critical or sensitive information, or made reference to the identification and protection of business-critical or high value equipment, or the safeguarding of business-critical functions and operations.

- Q12.2 anticipated students would detail physical, procedural, operational and/or communications security but student responses were often limited to no more than how risks are mitigated and the identification of vulnerabilities.

Section B presents more demanding, longer answer questions.

- The most common single answer for Q18.1 was spear phishing, possibly due to this having appeared within a question in the only other live paper in January this year. Some students suggested pharming in their response but this response was not appropriate to this question and was not allowed.

- Students were more successful with Q18.2 when their explanation included reference to the employee not being mindful of the rules and procedures intended to safeguard email security; for example, some students recognised that not meeting the terms and conditions of the SLA would undermine its intentions, as would failing to report an action known to have created an issue, as would any employee creating a security issue of which they themselves were the sole cause.

- Q19 offered a maximum of 7 marks; no student achieved full marks, but both Centres did each have a number of students achieved more than half marks. Some students did well in

their discussion of unauthorised access to recognise that any premeditation or advance planning was likely to result in a more severe penalty.

- Q20, the final question on this paper, offered a maximum 15 marks; no student achieved full marks, but some students reached the upper band, and several more reached the top end of the middle band. Students do seem to have benefitted from the bullet points at the end of this question; these bullet points were added to enable students to focus on the key elements of this final, very challenging question in their response. It will be seen from the mark scheme that while Q20 offered a maximum of 15 marks, student responses were rewarded piecemeal and equitably, with a maximum of 5 marks available for responses appropriate to each of the three required elements: authentication, authorisation, and access control.

Mark Ranges and Award of Grades

Grade boundaries and cumulative percentage grades are available on the Results Statistics page of the AQA Website.

Converting Marks into UMS marks

Convert raw marks into Uniform Mark Scale (UMS) marks by using the link below.
UMS conversion calculator