**SIT735 : Network Communications Security**

**Assessment Task Two: Technical report (part A) and online presentation (part B)**

This document supplies detailed information on assessment tasks for this unit.

**Key information**

* Due: 20 August, 2018
* Weighting: 30% (20% report; 10% online presentation)
* Word count: 2,000 words (technical report)

**Learning Outcomes**

This assessment assesses the following Unit Learning Outcomes (ULO) and related Graduate Learning Outcomes (GLO):

|  |  |
| --- | --- |
| **Unit Learning Outcome (ULO)** | **Graduate Learning Outcome (GLO)** |
| **ULO1** – Describe approaches to computer security including access control, identity verification and authentication in order to minimise cyber attacks on a system.  **ULO2** – Compare and contrast different types of cryptography including current cryptographic algorithms and their applications.  **ULO3** – Apply principles of public key cryptography to achieve secure communication networks by using digital certificates and digital signatures in compliance with industry standards. | **GLO1** – through the assessment of student knowledge of IT security and attacks to real-world systems  **GLO2** – through the assessment of student capacity to communicate technical findings and solutions with peers using appropriate language and professionalism.  **GLO4** – through the assessment of student ability to critically analyse information to propose feasible solutions  **GLO5** – through the assessment of student ability to use available IT techniques to protect computer systems. |

**Purpose**

This assessment allows you to develop an ability to explain approaches to computer security including access control, identity verification and authentication in order to minimize the cyber-attacks on a system.

You will need to investigate and choose the appropriate security tools to improve the security of a given system.

You will be assessed on your ability to collect security information based on the real world scenario described below, analyse the gathered information and propose feasible solutions with appropriate justification.

**Instructions**

The scenario:

It is 2011. You are working for one of the following three organisations:

* SME which deals with personal information
* Contractor who sets up networks for multiple small businesses (ie, you have a series of small clients whose security you maintain on a contractual basis)
* A reseller of certificates from a certificate authority.

News has just broken of the Comodo Certificate Authority Fraud Hack. Recent news suggest that a hacker may have obtained legitimate web certificates that would have allowed him to impersonate some of the top sites on the internet, including the login pages used by Google, Microsoft and Yahoo e-mail customers. Are your systems vulnerable, and what could be done to respond?

***Task A: Technical report***

Develop a technical report on up to 2,000 words based on the scenario described above.

You will need to research the Comodo certificate fraud hack in detail, isolate the risks that it presents to your clients/company and explore the security issues these present.

You’ll then need to provide an analysis of how to guard against the security issues you have identify and present feasible solutions. You must also provide a solid justification of these solutions.

While everything you need to solve the problem will be touched on during the course, it is expected that you will seek additional, high quality information to justify and give weight to your findings. The Library’s [Information Technology Resource Guide](http://deakin.libguides.com/infotech?hs=a) is a good place to start.

See the rubric for further details.

**Structure**

Your technical report should consist of the following:

|  |  |  |
| --- | --- | --- |
| Section | Content | Suggested word count |
| Cover letter | Title of report, your student number | Not counted towards final word count |
| Executive summary | A brief overview of the report | 150 words |
| Introduction | Background information including an overview of the scenario, aims of investigation. | 100 words |
| Body | Provide a description of the IT security problem, the major security problems it proposes and proposed solution. | 1500 words |
| Conclusion | A summary of your report, discussing the importance of the proposed solution. | 100 words |
| Recommendations | A concise list of actions that your company/client should undertake | 150 words |
| References | A list of any information the student has drawn on throughout the report | Not counted towards final word count |
| Appendices | Any information (graphs, charts, tables or other data) referred to in your report but not included in the body. | Not counted towards final word count |

A technical report aims to solve a problem and/or recommend a design. See

<http://www.deakin.edu.au/students/studying/study-support/academic-skills/report-writing> for further details.

***Task B – Oral (online) presentation***

You will need to develop and deliver a presentation on the findings of your report. You should prepare a ten minute presentation and expect to spend five minutes following answering questions.

Your presentation must include an introduction, a description of the IT security problems you’ve uncovered and your recommendations to solve the problems.

**Format:**

**Option A:** Your presentations will be delivered during online seminars in Weeks 5 and 6. Further details on which seminar you will present at will be made available during the trimester.

**Option B:** Your presentation will need to be made via Skype, Google Hangouts or an online conferencing technology as agreed between you and teaching staff. Please negotiate an appropriate date and time for the conference to occur. The last date on which your conference can be held is August 27th, unless otherwise agreed to with teaching staff.

**Submission details**

<mandatory>

**Extension requests**

Requests for extensions should be made to Unit/Campus Chairs well in advance of the assessment due date. Please follow the link for detailed information and form: <insert link if required>

**Special consideration**

You may be eligible for special consideration if circumstances beyond your control prevent you from undertaking or completing an assessment task at the scheduled time.   
See the following link for advice on the application process: <http://www.deakin.edu.au/students/studying/assessment-and-results/special-consideration>

**Assessment feedback**

You will receive feedback on your report and presentation in the form of a marking rubric no later than two weeks following your presentation.

**Referencing**

You must correctly use the Harvard in this assessment. See the Deakin [referencing guide](https://www.deakin.edu.au/students/studying/study-support/referencing).

**Academic integrity, plagiarism and collusion**

Plagiarism and collusion constitute extremely serious breaches of academic integrity. They are forms of cheating, and severe penalties are associated with them, including cancellation of marks for a specific assignment, for a specific unit or even exclusion from the course. If you are ever in doubt about how to properly use and cite a source of information refer to the referencing site above.

Plagiarism occurs when a student passes off as the student’s own work, or copies without acknowledgement as to its authorship, the work of any other person or resubmits their own work from a previous assessment task.

Collusion occurs when a student obtains the agreement of another person for a fraudulent purpose, with the intent of obtaining an advantage in submitting an assignment or other work.

Work submitted may be reproduced and/or communicated by the university for the purpose of assuring academic integrity of submissions: <https://www.deakin.edu.au/students/study-support/referencing/academic-integrity>

**SIT735: Network Communications Security**

**Assessment Task 2: Technical report rubric (PART A)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **High Distinction**  (80 – 100) | **Distinction**  (70 – 79) | **Credit**  (60 – 69) | **Pass**  (50 – 59) | **Fail**  (0 – 49) |
| **Collection of information**  10%  How relevant and comprehensive is the information you’ve collected? | The student has demonstrated a comprehensive and exceptionally well researched background and solution to the IT security problem, based on an extensive reading of relevant material. | The student has demonstrated a solid and well researched background and solution to the IT security problem, based on a wide range of readings. | Collects enough information to describe the background to, and provide a sound proposal for, a solution to the IT security problem. | Identifies bare minimum information required to provide a solution to problem. | Not enough relevant information has been identified to provide a solution to the problem. |
| **Analysis of information** 30%  How appropriate is your analysis of the information? | The analysis provided is exceptionally strong.  The analysis is novel and demonstrates in depth reflection on the causes and potential solutions to the problem, fully integrating the institutional contexts of the problem to the solution. | The analysis provided is strong.  The analysis explains the causes of the problems, and compares and contrasts potential solutions.  It explains how the institutional context, problem and solution are inter-related. | The analysis provided is sound. It describes the IT problems and provides a sound outline of the solution.  It describes how the solution to the problem is appropriate to the institutional context. | The analysis provided is very basic. It is enough to produce a simple identification or list of IT security problems and solutions to these problems. | No analysis has been provided, or the analysis is erroneous or insufficient to identify and solve the IT security problem. |
| **Feasibility of solution**  30%  How feasible is the solution you have proposed? | The solution is exceptionally well suited to solving the problem in the context of the organisation. The solution will solve the problem comprehensively and elegantly. | The solution provided is robust and strong. The student‘s solution has been carefully selected to take into account the organisational context. | The solution provided is sound. The student describes how it could be implemented in the context of the organisation. | The solution provided is very basic, and may help solve the basic underlying problem. | No solution has been provided, or the solution is infeasible. |
| **Justification of solution**  30%  How strong is you justification your proposed solution? | The solution has been comprehensively justified. A very strong argument has been presented regarding the appropriateness of the solution to the organisation. | The student provides a robust justification of why the solution is appropriate to the problem and the context of the organisation. | The student provides a description of why the solution is appropriate to the problem and the context of the organisation. | The student identifies why the solution is appropriate to the problem. Some relevant details may be missing. | No justification of solution is provided, or the justification is wholly unsound. |

**Assessment Task 2: Online presentation rubric (PART A)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **High Distinction**  (80 – 100) | **Distinction**  (70 – 79) | **Credit**  (60 – 69) | **Pass**  (50 – 59) | **Fail**  (0 – 49) |
| **Preparation**  10%  How relevant and comprehensive is the information you’ve collected? | Student is exceptionally well prepared for the presentation. | Student is well prepared for the presentation. | Student is adequately prepared for the presentation. | Basic preparation has been undertaken, but appear to have been rushed. | The student is not prepared for their presentation or has been difficult to communicate with to arrange the presentation. |
| **Visuals**  40%  How appropriate is your analysis of the information? | The visuals are relevant, attractive, engaging and are absolutely integral to the presentation. | The visuals are helpful, well-developed and add a great deal to the presentation. | The visuals have been developed with some thought and add to the presentation. | Visuals are present, accurate and do not distract from the presentation. | Visuals are not present, inaccurate or distract you from the presentation. |
| **Presentation**  40%  How feasible is the solution you have proposed? | The presentation is relevant, exceptionally strong, engaging and well delivered.  They respond to questions without dissembling. Their response is strong and comprehensive. | The presentation is relevant, robust and is well delivered.  Their response to questions is strong. | The presentation is relevant, sound and delivered without too many issues.  Their response to questions are sound. | The presentation gives a basic description of the content of the report and is possible to follow, with some effort.  Their response to questions is basic, but adequate. | The presentation does not relate to the problem or solution described in the report or is difficult to follow.  They cannot provide reasonable answers to questions. |
| **Timing**  10%  How strong is you justification your proposed solution? | The presentation went to within one minute either side of the designated time. | The presentation went more than two minutes over or under time. | The presentation went more than three minutes over or under time. | The presentation went more than four minutes over or under time. | The presentation went more than five minutes over or under time. |