Cardiff School of Computer Science and Informatics

Coursework Assessment Pro-forma

Module Code: CMT116
Module Title: Cybersecurity and Risk Management
Lecturer: Amir Javed & Yulia Cherdantseva
Assessment Title: Portfolio -Coursework 2
Assessment Number: 2
Date Set: 9th November 2021
Submission Date and Time: **18th January 2022 by 09:00 am via Turnitin**
Return Date: 18th February 2022

This assignment is worth 90% of the total marks available for this module. If coursework is submitted late (and where there are no extenuating circumstances):

1. If the assessment is submitted no later than 24 hours after the deadline, the mark for the assessment will be capped at the minimum pass mark.
2. If the assessment is submitted more than 24 hours after the deadline, a mark of 0 will be given for the assessment.

Your submission must include the official Coursework Submission Cover sheet, which can be found here:
https://docs.cs.cf.ac.uk/downloads/coursework/Coversheet.pdf

Submission Instructions

Your submission **MUST**

1) Include the Coursework Submission Cover sheet as the first page (this does not count towards the total page number/word count)
2) Include a title page (this does not count towards the total page number/word count) with your Student ID and Name
3) Include your name and student ID in the header or footer of all pages.
4) Properly reference any source that you used.

Coursework will consist of two parts. Part one will be a group report and part two will be an individual report. At the end of the coursework, you are required to submit **TWO** reports via **Turnitin**.

1) An individual report of no more than 1500 words. This includes references, diagrams, etc.
2) A group report of no more than 2000 words submitted by the group leader via Turnitin. This includes references, diagrams, etc.

It is your responsibility to check that your submission has been received successfully **before** the deadline. If there are any difficulties with the submission process, you **MUST** e-mail the module leader Amir Javed (JavedA7@cardiff.ac.uk) before the deadline. Include your submission in the e-mail and use the following subject line in your e-mail:

"CMT116 Coursework Submission Problems".

Report	Description		Type	Name
Individual	Cover sheet + Submission	Compulsory	One PDF (.pdf)	file CMT116-[student number].pdf

Group Report	Cover sheet + Submission	Compulsory	One PDF (.pdf)	file CMT116-[Group number-Student number of submitting group member].pdf

Any deviation from the submission instructions above (including the number and types of files submitted) will result in a mark of zero for the assessment.

Staff reserve the right to invite students to a meeting to discuss coursework submissions

Assignment

Scenario

A small family-owned book shop has decided to offer online purchasing. With the addition of an online bookstore, the company aims to reach a broader audience and increase book sales. The website will enable customers to create an account, store their credit card information for future purchases, keep track of their purchasing history, and deliver books anywhere within the UK and Europe.

Having heard of numerous companies falling victim to cyberattacks, the company have decided to hire "Secure Applications Ltd", a security consultant, to test its web application for vulnerabilities. During their investigation:

1) The security analyst found that by inserting a ***single quotation*** in any of the user input field on the user login Webpage resulted in an error message. They also discovered that an injectable SQL statement can be built by entering statements like ***OR '1'='1' - -*** in the user input field.
2) The security analyst was able to access files stored on the server and was able to load a remote script and execute it.
3) The security analyst observed that whenever they entered the line **"<script>alert('xss');</script>** " in the *product search* text box, an alert pop up appeared.

In terms of existing security measures taken by the company to protect itself from cyber-attacks, the analyst observed anti-virus software was installed on the company server, and each employee was issued an access card. Furthermore, they observed that all the servers used to host the website are kept in a room that all staff have access to.

Coursework

Coursework will consist of two parts. Part one will be group work submitted as a single group report, and part two will be an individual report. At the end of the coursework, you are required to submit two reports, an individual and a group report via Turnitin. The individual report needs to be submitted by everyone whereas, the group report can be submitted by one person on the team.

Part 1

(50%)

1) As a group discuss why risk assessment is required when developing an effective security policy. Then choose a risk assessment methodology to conduct qualitative risk analysis on all the threats identified to highlight the top five threats, based on risk arising from them, that the company is facing and propose the most appropriate methods to handle these risks. Based on your research, produce a report for the management on the viability of new business expansion, including how the company should handle the risk arising from a web application. Finally, create a security policy that the company should implement to protect itself from cyber-attacks. As a group submit a single report of not more than 2000 words along with an Appendix (recording minutes of all meeting) to your report. The Appendix should record the interaction that has taken place between group members – as minutes of any meetings that have taken place. The group report should contain
    a. Explanation on why risk assessment is required and justification on the choice of risk assessment methodology. (15%)
    b. Qualitative risk analysis to identify the most pertinent threats (25%)
    c. How should the company handle the top five risks? (15%)
    d. Design of information security policy to implement the risk mitigation strategy (35%)
    e. Appendix with minutes of meetings that have taken place between group members (10%)

Please note: For the group report, a uniformed mark will be given to the group, that is each group member will be given the same mark. Group members must appoint a group leader who will ensure that work has been distributed equally, and it has been clearly recorded in the minutes as to which team member is doing which task. If a team member has made **NO** contribution towards the group report, the minutes of the meeting would be used as evidence and marks for that individual will be decided separately from the group mark.

Part 2

(50%)

2) Due to Covid-19 there has been a rise in mobile collaborative working, and network de-perimeterisation. As a result, existing security technologies may no longer be sufficient to secure data effectively. Providing with a minimum of one and no more than three supporting examples, write an individual report of no more than 1500 words to
    a. Discuss risks to data in these environments (35%)
    b. The limitations of existing security technologies, (35%)
    c. Your recommendations for addressing these. (30%)

Please note: Your work will be checked for collusion and plagiarism both automatically and manually. Any suspicion of Academic Misconduct will be reported to the Academic Misconduct Coordinator and could result in you being subjected to the Academic Misconduct Procedure. If you are found guilty, consequences may include a mark of zero for the coursework as well as exclusion.

To avoid this, keep in mind:

1. Do not copy material from other authors.
2. Properly reference all external material you use. Employ either the Cardiff Harvard Referencing style or any other style common in Computer Science (e.g. an ACM citation style), but be consistent throughout.
3. If you are in doubt whether you may be committing Academic Misconduct, please check the University's guidelines on referencing and contact your personal tutor and/or the module leader.

Learning Outcomes Assessed

1. Determine, establish and maintain appropriate information security regulations for an organisation.
2. Identify, analyse, evaluate and manage risks related to different components of an information system (i.e. data, people, processes, hardware, software and network) accounting for current threat landscape
3. Identify and effectively articulate different types of threat to, and vulnerabilities of, information systems to a range of audiences (e.g. top management, end users, non-technical and technical experts)
4. Critically analyse a wide range of security countermeasures, select and justify appropriate security countermeasures to mitigate risks by calculating return on security investment and economic impact of a security-related incident on business.
5. Effectively evaluate and apply popular risk assessment methodologies and information security management frameworks to case studies.
6. Define and implement effective security policies and processes within an organisation, make and sustain argument; make judgement and propose solutions

Criteria for assessment

Credit will be awarded against the following criteria (equal weighting):

1. Knowledge and understanding – ability to demonstrate knowledge of the subject and ability to apply theory in a critical and thoughtful way.
2. Evidence and Analysis - demonstrates an ability to construct a very well justified argument or position on the basis of appropriate evidence.
3. Reading and Research - evidence of the ability to read widely and make effective use of reading to support arguments.
4. Presentation Mark - sure your presentation is clear, concise, and well structured. It must be possible to understand the basics of your solution through a single reading.

Mark Range	Knowledge & Understanding	Evidence & Analysis	Reading and Research	Presentation
85 – 100%	Outstanding subject knowledge. Excellent understanding of different recent debates and key issues in topic area under investigation.	Demonstrates an ability to construct a very well justified argument or position on the basis of appropriate evidence. Demonstrates an ability to evaluate a wide range of relevant material.	Evidence of the ability to read widely and make effective use of reading to support arguments. Demonstrates an ability to research for information independently and to read critically.	Clear and articulate writing style with no spelling or grammatical errors. Complies with presentation criteria. Accurate referencing within the text and clear acknowledgement of sources used. Accurate and complete bibliography.
70 – 84%	Wide knowledge of subject and ability to apply theory in a critical and thoughtful way. A thorough understanding of different debates and key issues in topic area under investigation.	Strong evidence of the ability to make a sustained argument or position based on appropriate evidence. Shows an ability to evaluate the evidence and synthesise material to form a coherent discussion.	Evidence of the effective use of a wide selection of appropriate material. Uses evidence from research to support arguments. Strong evidence of independent research and some critical reasoning.	Clear and engaging writing style that demonstrates very good command of English. Complies with presentation criteria, accurate referencing within the text and clear acknowledgement of source used.
60 – 69%	Very good subject knowledge and understanding of key issues and debates in topic area under investigation. Evidence of a good understanding of relevant theoretical material.	Evidence of the ability to make a sustained and coherent argument using appropriate evidence. Evidence of ability to evaluate the evidence and synthesise generalisations.	Evidence of appropriate reading and ability to use a range of sources effectively to support arguments. Evidence of independent research.	Clear writing style that demonstrates a good command of English. Few imprecise statements. Adheres closely to presentation criteria. Referencing mostly clear and accurate.

50 – 59%	Sound subject knowledge and understanding of key issues and debates in topic area under investigation. Evidence of understanding some of the relevant theoretical material relevant to the assessment task.	Evidence of the ability to construct an argument using appropriate evidence. Evidence of an ability to collate information and reach some general conclusions. Evidence of a satisfactory level of analysis of theoretical issues	Evidence of ability to select appropriate material from different sources and to develop a coherent argument. Satisfactory deployment of evidence to support argument. Some evidence of independent research.	Correct English usage with few imprecise statements. Adheres to most aspects of presentation criteria and clear attempts made to acknowledge sources accurately within the text.
49 – 1%	Evidence of some understanding of appropriate theory, but lacking depth. Limited understanding of key issues and debates in topics under investigation.	Some evidence of analysis of relevant material but with limited argument and evidence. Evidence of the ability to construct a coherent response to the assessment task, but only a basic level of interpretation and evaluation	Evidence of selection of mainly relevant material from a wide range of sources, but evidence may not be deployed accurately. Narrow selection of material and/or limited evidence of independent research.	Correct English usage, but with some lack of precision. Some aspects of the work are not explained clearly and marks limited by the material that the marker can understand. Presentation criteria may not be wholly adhered to. Referencing and bibliography attempted but may lack accuracy.
0	Cheating (including plagiarism, collusion, duplication and falsification). Submitting other people's work as your own. Failing to present work.			

The following gives an indication of the level of attainment against the appropriate award:

Distinction (70-100%)

Merit (60-69%)

Pass (50-59%)

Fail (0-50)

Marks will be assigned as indicated in the Assignment Description.

Marking Guide	
Individual Report	50%
Group report (one mark to a group)	50%

Feedback and suggestion for future learning

Feedback on your coursework will address the above criteria. Feedback and marks will be returned on 18th February 2022 via Turnitin.