Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	Student fill in own ID and attach document for submission

Module Title & Code	WM140 Cyber Systems Architecture and Organisation
Module Owner	Amila Perera
Module Tutor	
Module Marker	Amila Perera
Assessment type	Coursework
Date Set	06/12/2021
Submission Date (excluding extensions)	07/03/2022 (refer to Tabula)
Marks return date (excluding extensions)	(Refer to Tabula)
Weighting of mark	100%

Assessment Detail	See below
Word Count	Section A Part I – There is a 600-word limit for this part. Section A Part II – There is a 600-word limit for this part. Section A Part III – There is a 600-word limit for this part. Section B Part I and Part II – There is no limit for this section. There is a 10% margin on the word count. Excessive length may be penalised, and the marker may ignore any material over the word limit. The word count includes footnotes and tables but excludes references and appendices.

<table>
<tr><td>Module learning outcomes (numbered)</td><td>1. Explain the relationship between the abstractions used to represent programs and data, and their concrete representation on real machines.
2. Explain the relationship between the key architectural components of a modern, multicore processor.
3. Evaluate code at the assembly language level to analyse cyber consequences from insecure patterns of code.</td></tr>
<tr><td>Learning outcomes assessed in this assessment (numbered)</td><td>1. Explain the relationship between the abstractions used to represent programs and data, and their concrete representation on real machines.
2. Explain the relationship between the key architectural components of a modern, multicore processor.
3. Evaluate code at the assembly language level to analyse cyber consequences from insecure patterns of code.</td></tr>
<tr><td>Marking guidelines</td><td>
<table>
<tr><th>Criteria</th><th>Mark</th></tr>
<tr><td>Section A</td><td></td></tr>
<tr><td>Part I: Relevant discussion with appropriate justifications</td><td>20</td></tr>
<tr><td>Part II: Relevant discussion with appropriate justifications</td><td>20</td></tr>
<tr><td>Part III: Relevant discussion with appropriate justifications</td><td>20</td></tr>
<tr><td>Section B</td><td></td></tr>
<tr><td>Part I: Clear Illustration of the step-by-step approach with appropriate justifications</td><td>20</td></tr>
<tr><td>Part II: Relevant discussion with appropriate justifications</td><td>10</td></tr>
<tr><td>Presentation</td><td></td></tr>
<tr><td>Report structure and references</td><td>10</td></tr>
<tr><td>TOTAL</td><td>100%</td></tr>
</table>
</td></tr>
<tr><td>Submission guidance</td><td>You must use the Harvard referencing system. All submissions should be made in PDF format. Please follow further guidelines on Moodle</td></tr>
</table>

Academic Guidance	*Academic guidance to be provided throughout the module.*
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of 5 marks per university working day after the due date, up to a maximum of 10 working days late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means after the submission deadline time as well as the date – work submitted after the given time even on the same day is counted as 1 day late.

Assessment Detail

Section A

I. A student argues that it is more challenging to perform a stack-based buffer overflow attack in a x86_64 system than a x86 system. Discuss your opinion about this statement using an example.

II. Discuss how modern computer systems mitigate buffer overflow attacks in multiple layers

III. Explain how side-channel attacks via CPU cache could affect the hardware security of computer

Section B

I. You have been given a binary file that expects the correct passphrase as the user input to display the “Access Granted” message. Explain how you could use gdb to trace through the code and bypass passphrase validation during the runtime.

II. Propose and justify an alternative solution to mitigate this weakness in the program implementation.