UNIVERSITY OF Hull

DEPARTMENT OF COMPUTER SCIENCE
ASSESSMENT DESCRIPTION 2019/20
(EXAM TESTS WORTH ≤15% AND COURSEWORK)

MODULE DETAILS:

Module Number:	700108	Semester:	1
Module Title:	Network Security		
Lecturer:	Brian Tompsett		

COURSEWORK DETAILS:

Assessment Number:	2	of	2		
Title of Assessment:	Network Protocol Security Flaws				
Format:	Report	2nd format	Presentation		
Method of Working:	Individual				
Workload Guidance:	Typically, you should expect to spend between	50	and	80	hours on this assessment
Length of Submission:	This assessment should be **no** more than: *(over length submissions **will be** penalised as per University policy)*	5000 **words** *(excluding diagrams, appendices, references, code)*			

PUBLICATION:

Date of issue:	6 November 2019

SUBMISSION:

ONE copy of this assessment should be handed in via:	Canvas		If Other (state method)	Demonstration
Time and date for submission:	**Time** *(must be before 4pm)*	2pm	**Date**	4 Dec 2019
If **multiple hand–ins** please provide details:	A powerpoint presentation should be made at a time assigned later			
Will submission be scanned via TurnitinUK?	Yes	If submission is via TurnitinUK students MUST only submit Word, RTF or PDF files. Students MUST NOT submit ZIP or other archive formats. Students are reminded they can **ONLY** submit **ONE** file and must ensure they upload the correct file.		

The assessment must be submitted **no later** than the time and date shown above, unless an extension has been authorised on a *Request for an Extension for an Assessment* form: search 'student forms' on https://share.hull.ac.uk.
Canvas allows multiple submissions: only the **last** assessment submitted will be marked and if submitted after the coursework deadline late penalties will be applied.

MARKING:

Marking will be by:	Student Name

ASSESSMENT:

The assessment is marked out of:	40	and is worth	30	% of the module marks
N.B If multiple hand-ins please indicate the marks and % apportioned to each stage above (i.e. Stage 1 – 50, Stage 2 – 50). It is these marks that will be presented to the exam board.				

ASSESSMENT STRATEGY AND LEARNING OUTCOMES:

The overall assessment strategy is designed to evaluate the student's achievement of the module learning outcomes, and is subdivided as follows:

LO	Learning Outcome	Method of Assessment *{e.g. report, demo}*
LO1	*Demonstrate a comprehensive understanding of the vulnerabilities of Networked Computers and their protocols*	Report, Presentation
LO2	*Provide evidence of research, selection and assessment of a range of mitigation techniques against vulnerabilities*	Report, Presentation
LO3	*Apply techniques for the Management and Configuration of Firewalls*	Report, Presentation
LO4	*Select, justify and apply a range of Network Management Protocols*	Report, Presentation

Assessment Criteria	Contributes to Learning Outcome	Mark
Report:		
- Range of protocols	LO1	5
- Explanation of flaws	LO2	5
- Suitable mitigation covered	LO3	5
- Overall Quality of report, writing and bibliography	LO4	5
Presentation:		
- Clarity of explanation		5
- Level of presentation		5
- Suitability for audience		5
- Overall Quality of slides and language		5

FEEDBACK

Feedback will be given via:	Verbal (via demonstration)	Feedback will be given via:	Annotation
Exemption (staff to explain why)			
Feedback will be provided no later than 4 'teaching weeks' after the submission date.			

This assessment is set in the context of the learning outcomes for the module and does not by itself constitute a definitive specification of the assessment. If you are in any doubt as to the relationship between what you have been asked to do and the module content you should take this matter up with the member of staff who set the assessment as soon as possible.

You are advised to read the **NOTES** regarding late penalties, over-length assignments, unfair means and quality assurance in your student handbook, which is available on Canvas - https://canvas.hull.ac.uk/courses/17835/files/folder/Student-Handbooks-and-Guides.

In particular, please be aware that:

- Up to and including 24 hours after the deadline, a penalty of 10%
- More than 24 hours and up to and including 7 days after the deadline; either a penalty of 10% or the mark awarded is reduced to the pass mark, **whichever results in the lower mark**
- More than 7 days after the deadline, a mark of zero is awarded.

- The overlength penalty applies to your written report (which includes bullet points, and lists of text. It does not include contents page, graphs, data tables and appendices). 10-20% over the word count incurs a penalty of 10%. Your mark will be awarded zero if you exceed the word count by more than 20%.

Please be reminded that you are responsible for reading the University Code of Practice on Academic Misconduct through the Assessment section of the Quality Handbook (via the SharePoint site). This govern all forms of illegitimate academic conduct which may be described as cheating, including plagiarism. The term ‘academic misconduct’ is used in the regulations to indicate that a very wide range of behaviour is punishable.

In case of any subsequent dispute, query, or appeal regarding your coursework, you are reminded that it is your responsibility, not the Department’s, to produce the assignment in question.

Network Protocol Security Flaws

INTRODUCTION

This assessment is for you to learn about the flaws in the protocols used in the internet and the mitigation used to prevent exploitation of those flaws. The lecture course included an introductory lecture on the topic of protocol flaws which will get you started. You should then perform your own reading and research to discover more details which you should put into a technical report. You should ensure that your report content is properly cited using the Harvard method used at the University of Hull and includes a comprehensive bibliography of your research reading.

In the security profession the ability to communicate detailed technical information to non-technical (perhaps executive) audience is useful, you should also prepare and present a PowerPoint presentation on your findings. The presentation should be targeted to be about 20 minutes in length.
The arrangements for the presentations will be advised nearer the time.

Your report should be written for a technical but non-specialist audience, such as a manager, academic or undergraduate student with no specialist knowledge of networks or security but skilled with computers. The report will be scanned by Turnitin.