School of Computer Science – Coursework Issue Sheet

Session	2018/19	**Semester**	2
Module Name	Computer Security	**Code**	G53SEC COMP3006
Module Convenor(s) **(CW Convenor in Bold)**	**Michael Pound**		

Coursework Name	Portfolio of Lab Work	**Weight**	40%
Deliverable (a brief description of what is to be handed-in; e.g. 'software', 'report', 'presentation', etc.)	Written report		
Format (summary of the technical format of deliverable, e.g. "C source code as zip file", "pdf file, 2000 word max", "ppt file, 10 slides max", etc.)	2000 word pdf submitted via moodle		

Issue Date	March 22th
Submission Date	Monday May 13th
Submission Mechanism	Via Moodle
Late Policy **(University of Nottingham default will apply, if blank)**	Default of 5% per working day.
Feedback Date	By May 28th
Feedback Mechanism	Written feedback via moodle.

Instructions	Instructions will be released on moodle.
Assessment Criteria	• Submissions will be assessed numerically, from 0 to 100% • The main assessment criteria for the report are: – Correctness – Is what you have written technically correct? – Analysis – Have you justified your decisions with background knowledge? – Completeness – Have you explored as many aspects of the subject as possible? – Presentation – Is the report well written?

G53SEC COURSEWORK 2018/2019 DEADLINE: 13TH MAY

INTRODUCTION

This coursework requires you to write a detailed report, of up to 2000 words, that covers three aspects of computer security you will have encountered in the labs and lectures. Marks will be awarded for the correctness and completeness of your answers, have you explored each topic in enough depth, and is what you have written about technically correct. For top marks, any additional knowledge or insight beyond what I have told you would demonstrate that you really understand the concepts.

QUESTION 1: PASSWORDS

For this question you are expected to write **up to 500 words**. A system administrator has asked you to design a new password and authentication policy for their network, and justify your choices. Given your experiences in the password labs and lectures, what password policy would you advise? In other words, what rules would you enforce on users for their passwords? These rules could involve constraints on the passwords, password use, expiration etc. Would you recommend any additional authentication measures, and in which cases? How would you suggest storing the passwords? Bear in mind that this policy would be rolled out to many users, so must be realistic as well as robust. Be sure to explain the reasoning behind each suggestion.

QUESTION 2: FIREWALLS

In this question you are expected to write **up to 500 words**. It has become commonplace to use permitted services such as SSH to "tunnel" traffic that would otherwise be blocked by a network firewall. Give some examples of reasons an administrator might choose to block ports from normal traffic. Describe in detail how a protocol such as SSH can be used to circumvent firewall restrictions. Give an example of a time when someone might use SSH tunneling for a perfectly legitimate reason, and one where someone might use it for more disreputable purposes.

QUESTION 3: SERVER SECURITY

This question requires you to write **up to 1000 words**. During the final lab you scanned and accessed a vulnerable server, and then worked to improve its security. Describe in detail what actions you performed, and why, and what actions you would perform if you had more time. Which services did you install or remove? What configurations did you change? And so on. As you can imagine, there are countless things you *could* do to this machine to improve security, try to perform or describe as many as you feel is reasonable to secure it. Many marks are available here for detail and justifications of your actions, but given you have 1000 words, try to priorities the critical vulnerabilities first. In some cases (e.g. distribution upgrades) it is acceptable to say what you would have done given more time, but feel free to perform these actions if you wish.