COMP3028 COURSEWORK 2018/2019

DEADLINE: 5pm, 3rd May 2019

INSTRUCTION: Answer ALL questions

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 (25 marks)

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? 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 your decisions. What attacks, for example, are you preventing with your password policy?

QUESTION 2: FIREWALLS (25 marks)

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. Describe in detail why an administrator might choose to block ports from normal traffic. Describe 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 (50 marks)

This question requires you to write **up to 1000 words**. During the final labs you worked to improve the security of a vulnerable server. 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, 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.

MARKING SCHEME (Marks in brackets are for Q3)

Category	Description	Marks
Correctness	Is what you have written technically correct?	10 (15)
Analysis	Have you justified your decisions with background knowledge?	5 (15)
Completeness	Have you explored as many aspects of the subject as possible?	5 (10)
Presentation	Is the report well written	5 (10)
Total		25 (50)

SUBMISSION INSTRUCTION:

Submit all reports in a **single** PDF file with clear headings to separate the questions. I suggest start a new page for each question. Remember to include your **word counts** and references.

Coursework FAQ

Is the word limit strictly enforced?

No. My rule is I will deduct marks if you write more than the word limit +10%. E.g. for the third question you will lose marks if you write more than 1100 words. I use this policy so that people don't obsess about word counts, e.g. 1001 words is fine, but just so people don't push it. It's perfectly possible to get a very high mark within the word limit.

Can I write fewer words than the word limit?

Yes! If you're confident you've answered the question then that's fine. Just be aware that if you've written 50% of the word limit, you likely haven't answered the question.

Is the machine we're securing in Question 3 *any* Ubuntu server, or the one from the labs?

The one from the labs. This is an important point, I'm not looking for info on in securing servers in general, I'm interested in what you discover about the Ubuntu lab machine's vulnerabilities, and how you address them. Be aware that if you don't run the Ubuntu lab VM and so don't answer Q3 properly, you will lose marks.

Can we work in pairs / teams?

You can discuss the coursework, you must submit individual work. I have no issue with people talking about the questions, and discussing security topics etc. - this is a good way to learn. *But*, write the document on your own. If you submit a document that contains text from another person's coursework, or is extremely structurally similar, you risk getting zero marks.