Systems Security 2018/19 Coursework

1. Outline

This year there will be four lab tasks split into two pieces of coursework. Each coursework is worth 30% of the unit mark and the remaining 40% comes from a final exam.

- Coursework 1 covers labs 1 and 2 (format strings and buffer overflows). These labs are in weeks 5 and 6 and Coursework 1 is due in week 7.
- Coursework 2 covers labs 3 and 4 (networks and SQL injection). These labs are in week 9 and 10 and Coursework 2 is due in week 11.

For each coursework, you will work in groups of 4. We will sort out groups before the labs begin. You will get an opportunity to form groups of your own by a deadline (to be announced in the lectures), after which I will randomly assign the remaining students to groups.

SAFE suggests that there will be over 80 students on the unit this year. Please understand that I do not have the time to create group assignments based on everyone's preferences with some kind of matching algorithm – you will get the opportunity to form your own groups of four, anyone not in a group by the deadline must work with whoever they get as their randomly assigned partner.

2. Technical and Reflective sections

For each lab, you must include two sections in your coursework:

- A *technical* section, describing what you did and how/why it works.
  Imagine that you are writing for another student who has not taken this unit: they should be able, after reading your technical part, to both reproduce your attacks by following the steps you give and to have a basic understanding of what is happening. You are also strongly encouraged to provide scripts to reproduce your attack (please check with the TAs how best to do so).

- A *reflective* section, in which you critically reflect on the circumstances (both technical and organisational) that can give rise to the relevant vulnerabilities and potential mitigations. This can include e.g. mention of real instances of these attacks that you have researched, comparison to other attacks, discussion of relevant standards and recommendations (CERT, OWASP etc.).
  You can also discuss topics relating to the vulnerabilities that you exploited, including: their potential risk and impact in real systems; why they (still) exist; which straightforward attempts at mitigation do not work and why not; how you would successfully reduce or eliminate these vulnerabilities.
  For the reflective section, you can imagine that you have been called in as a consultant

to a company whose systems have just been breached by the vulnerabilities in question. In the narrow sense, you need to fix the vulnerabilities – in a wider sense, you need to fix the company (culture) / *system* that let them appear in the first place.

3. Submission rules

To help with the marking process, in particular getting the marks and feedback back to you in good time, you must follow the rules in this section. Some of the rules are also designed to limit the amount of work you are expected to do for the coursework on this unit.

Please read the rules carefully – deviations that disrupt the marking process may result in losing marks.

3.1 General rules

- For each coursework, you must submit two pdf files, one containing the technical sections and one containing the reflective sections. The names of the files should make clear which is which.
- You must submit PDF files, not text files, word documents, JPEGs of scanned documents, TeX sources etc.[1] Anything else will receive 0 marks. Exception: if you wish to submit scripts or other code along with your PDF reports for certain tasks, you may do this.
- Marking will be anonymous. You must include the candidate numbers (5-digit numbers, NOT your usernames) of both group members clearly visible on the first page of every PDF document that you submit and you must not include personally identifying information such as your real name or university username anywhere.

3.2 Reflective sections

For the reflective sections, you must submit a PDF file with exactly 4 pages[2] per coursework:

- Pages 1-2 must contain the reflective section for the first lab.
- Pages 3-4 must contain the reflective section for the second lab.
- Your candidate numbers must be included on at least pages 1 and 3.
- Your font size and page margins must be reasonable (I may want to make small notes in the margins).

This means a strict limit of 2 pages for each reflection including any references, images etc. (you are of course welcome to write shorter reflections than this). You will lose points if you exceed the limit, and the extra page(s) will be ignored.

The reason for these rules is so that I can print all reflections, easily sort them into "lab 1" and "lab 2" piles and then mark them efficiently together with my TAs while trying my hardest to

[1] In past years and on different units Submissions have included a .docx file with the file extension changed to .pdf and a .tex file with a comment "sorry it doesn't compile". Both of these received 0 marks.
[2] A page is a single side of a two-sided sheet of paper.

make the assignment and marking scale the same for everyone, be able to cross-check marks for consistency at the end and still get everything marked (I hope) within 3 weeks.

Each reflection will be marked out of 10 according to the M-scale (i.e. 7/10 is already "excellent"). Minor violations of the page limit rule will result in a penalty of 0.5 marks. You will receive written feedback on your reflections, uploaded as a text file to SAFE.

3.3 Technical sections

There is no strict limit for these but don't go overboard. I suggest an upper limit of 4 pages per lab. Anything over 8 pages (including images, references) is probably excessive for most of the labs.

Do not take any screenshots of terminals: instead, copy and paste the text and format it in a monospace font.

You will receive a mark out of 10 for each technical section and feedback in a text file uploaded to SAFE.

3.4 Work distribution

All group members are responsible for all the submitted work. Only one member of each group needs to submit to SAFE. I hope that in most groups, the work distribution will be 25% for each group member; if this is not the case then you may indicate the distribution on the first page of your technical section's PDF file in the following format:

Work distribution: (candidate number 1) X %, (candidate number 2) Y %

You may not assign individual sections to different group members: all group members are responsible for all sections.

3.5 Plagiarism

Plagiarism is normally not much of a problem on the MEng cohorts, nonetheless please remember and follow the following rules and ask me if there are any questions about this.

- Your coursework that you submit must be your own group's work.
- Any material you use must be properly referenced/cited.
- Direct quotes from sources must be marked as such. For text, this generally means place it in quotation marks and reference it; for code, include a comment at the top of the file or function in question indicating the source; for images/figures this means put something like "source: (reference)" as a legend below the image.
- Under no circumstances can you copy from other groups' reports.

The SEED labs that we use are a well established teaching tool and there are Q&A and sample solutions to them on the internet. You are allowed to read and reference material on the internet like any other sources, and you are strongly encouraged to do your own further research and reference things that you found in your reports.

4. Marking and feedback

In a masters-level unit, you are expected to demonstrate evidence of research and reflection beyond the material taught in the lectures and labs in order to obtain a top grade. Doing everything on the exercise sheet correctly to the letter should get you 65%; marks above that are for contributions beyond the expected minimum in terms of quality.

Quality is more important than quantity; a report that makes a point well in one page is better than one that does the same task in four pages but does not highlight the important points or have a clear structure. The worst thing you can do is spend hours and hours writing a 50-page report that tries to deal with everything including the kitchen sink, but ends up being poorly structured and missing the key points of the attacks in question. It won't get you a high mark and it's a waste of your time (each section is worth 0.625% of your final year).

The following are examples of quality:

- attack descriptions and explanations that are both clear and concise
- explaining how one could develop the attacks further, or apply similar techniques to other vulnerabilities
- effectively combining the "what" and the "why" of the attacks
- referencing relevant material outside of the unit resources
- real-world examples of instances of the attacks discussed
- good writing style and structure
- highlighting the key concepts involved
- categorising the attacks/vulnerabilities and placing them in a larger context or comparing with other attacks
- assessing the prevalence, impact/severity or the difficulty of mitigating a class of attack – with supporting evidence (e.g. references to OWASP or similar vulnerability classification resources)
- individual contributions of your own that I have not thought of here, but that are relevant to the vulnerabilities/attacks being discussed

Each group will receive individual, written feedback on all tasks. I hope to be able to return all feedback within the university guideline of 3 weeks from the submission date.

The reflective and technical sections carry equal weight so each of the two sections of each lab is worth 7.5 % of the unit mark (since each coursework is worth 30% and has two labs with two sections each).

The tasks I've asked you to do cannot be marked simply by checking how many boxes of a standardised marking sheet you've ticked. You deserve feedback of at least the same quality as the coursework that you hand in, and that means I will read each and every one of your reports in detail – which I'm happy to do, but it also means I cannot absolutely guarantee feedback by a fixed deadline.