FAILY, S. 2014. Ethical hacking assessment as a vehicle for undergraduate cyber-security education. In Uhomoibhi, J.O., Linecar, P., Barikzai, S., Ross, M. and Staples, G. (eds.) *Global issues in IT education: proceedings of the 19th International conference on software process improvement research, education and training (INSPIRE 2014), 15 April 2014, Southampton, UK*. Southampton: Solent University, pages 79-90.

Ethical hacking assessment as a vehicle for undergraduate cyber-security education.

FAILY, S.

2014

Ethical Hacking Assessment as a Vehicle for Undergraduate Cyber-Security Education

Shamal Faily[1]

[1]Software Systems Research Centre, Bournemouth University,
Fern Barrow, Poole BH12 5BB
sfaily@bournemouth.ac.uk

Abstract

The need for cyber security professionals in the UK is growing, motivating the need to introduce cybersecurity at an earlier stage of an undergraduate's education. However, despite on-going interest in cybersecurity pedagogy, there has been comparatively little work exploring the role of assessment in educating future cybersecurity practitioners. This paper presents a case study on the re-design and critical evaluation of an undergraduate ethical hacking coursework assignment. The study describes how recent work in ethical hacking pedagogy informed an assignment re-design, and the revised assignment was critically analysed based on constructive alignment, student engagement, and plagiarism.

1.0 Introduction

Based on recent government reports [1], the number of cyber security professionals in the UK has not increased in line with the growth of the Internet. The resulting career prospects have attracted students to security-focused undergraduate programmes around the UK, including the Forensics & Security programme at Bournemouth [2]. To develop these programmes, institutions have repurposed cybersecurity teaching material -- traditionally consigned to professional and postgraduate education -- to the formative stages of undergraduate courses. As a result, despite the growing body of cybersecurity pedagogy, this needs to be critically analysed to determine its appropriateness for an undergraduate audience.

One of the lesser-explored areas of cybersecurity pedagogy is assessment. Assessment shapes the experience of students more than the teaching they receive, with many students choosing to delay their engagement with teaching material until faced with assessment tasks [3]. Given both the need to adapt teaching material for undergraduates, and the relatively unexplored impact of assessment in cybersecurity education, a case study on the re-design and evaluation of a coursework assignment for Bournemouth University's Ethical Hacking & Countermeasures unit is presented. This assignment builds on recent lessons learned in cybersecurity pedagogy, and addresses weaknesses in the previous coursework assignment template. To provide context to this assignment, some current tensions in cybersecurity education are described, before cybersecurity education at Bournemouth is summarised, together with recent findings designing and applying cybersecurity assessment. The previous year's assignment is reviewed before presenting the revised assignment design. The paper concludes by critically analysing the revised assignment from three different perspectives: constructive alignment, student engagement, and plagiarism.

2.0 Background

2.1 Tensions in Cyber Security Education

It is accepted that cybersecurity should be on the educational curriculum, and there is growing debate on how to progress cybersecurity pedagogy [4], particularly in ethical hacking [5, 6, 7]. There are, however, tensions about the perspective to take when teaching cybersecurity at universities. Schneider [8] claims that addressing these tensions are central to developing an effective cybersecurity course.

Some institutions argue that cybersecurity courses should teach adversarial thinking; students should be taught specific attacks, in the hope that they can generalise from this material and learn how violating assumptions can lead to insecurity or, based on the "Lock maker'" metaphor, learning how to break locks helps students make better locks [9].

Other institutions believe that disassembling artefacts and finding insecurity does not imply education on building security into the design of systems. Courses taking this perspective teach security principles and use case studies that demonstrate their application. However, to evaluate such systems, adversarial thinking remains necessary.

2.2 Cybersecurity Education at Bournemouth

Undergraduate cybersecurity education at Bournemouth is initially delivered to students via two mandatory course modules: Digital Forensics and Ethical Hacking & Countermeasures. The Digital Forensics course teaches students how to carry out a forensic analysis of computer artefacts using a range of software tools. The

Ethical Hacking & Countermeasures course, which this paper is concerned with, teaches students how to "hack" into computer systems to evaluate their security. Together, these course modules provide opportunities to learn about a variety of practical topics in cybersecurity.

Both course modules are delivered simultaneously to Level I (second year) Computing undergraduates. These students have broad technical experience, but start both courses lacking the detailed expertise necessary to both forensically analyse computing systems, and evaluate their security. The course modules provide a vehicle for developing this expertise, but students find the skills learning curve steep. However, as students expect to apply this expertise in industrial placements in their 3rd year, overcoming this learning curve is essential.

2.3 Ethical Hacking & Countermeasures

The Ethical Hacking & Countermeasures (EHC) course is a "long and thin" module delivered over a 20-week period across two semesters. Each week, students receive a one-hour lecture, and a two-hour lab. The course is vocational in nature, and closely aligned to the commercially recognised role of *penetration tester*, which has an associated industry accreditation [10].

The EHC curriculum is broad; course topics range from security principles and cyber ethics, to network penetration testing and malware analysis. The broadness of the curriculum makes student engagement challenging, particularly as the course marks their first encounter with cybersecurity theory. The engagement problems are evident because many students initially question the relevance of security principles taught in the formative weeks of the course. As a result, they fail to connect this theory with topics taught later. This is particularly evident with the material taught on cyber ethics, based on the difficulty many students face when evaluating the ethical implications of network penetration classes later in the course.

The EHC course is assessed by two tasks: a coursework assignment and an invigilated examination; each task accounts for 50% of the overall mark. The invigilated exam takes place at the end of the second semester and broadly assesses the non-practical elements of the course. The coursework assignment primarily assesses technical skills that cannot be evaluated in the exam. This assignment is issued half way through the academic year, and students are given roughly two months to complete it.

2.4 Assessing Ethical Hacking

Several studies have considered the design of ethical hacking courses, but there has been almost no work focusing on the design of their assessment tasks. More recently, however, two studies have considered assessment task design for such courses.

In their case study on running cybersecurity attack and defence laboratories, Standard et al. [11] issued homework assignments for each associated class. The final examination also included questions based on content covered in the class

exercises. Although the marks received by students indicate that this approach was effective, such an approach may be problematic when applied to the ethical hacking course at Bournemouth for two reasons. First, participants on this course attend pre-requisite cybersecurity courses. This means students are less likely to wrestle with theory while also understanding how to apply skills in practice, ensuring homework assignments are completed faster. Second, although the course runs for approximately the same period, the course includes twice as many lectures per week, and multiple demonstrators per class; this extra support means that theoretical deficiencies that might not become apparent until completing the homework can be rectified in class.

Dimkov et al. [9] describe an assignment designed for an introduction to computer security course for postgraduate students. The assessment incorporated two elements: writing a scientific paper, and completing a practical assignment. The practical assignment required students to steal a laptop, decrypt data found on the laptop, and carry out an attack on a vulnerable machine. Such an assessment strategy may be difficult to implement precisely as part of the EHC course for three reasons. First, the assignment involves deception and, as such, would need to be subject to the university's own ethical approval processes. Such an application is unlikely to be successful without the students first receiving explicit training on working with human subjects in experiments, which they do not have time to complete. Second, such an assessment requires students to work in teams. While realistic, assessing the contributions that individuals make becomes challenging. Third, Dimkov et al. acknowledge that such assignments are difficult to run over multiple years because it becomes harder to social engineer people that may be aware that such an assessment is taking place.

3.0 Coursework Design

3.1 Existing Coursework Design

The coursework assignment for the 2012-2013 academic year asked students to plan, conduct, and document four exploits of their choice. The assignment was open-ended in that it gave substantial flexibility for students, particularly those less technically capable, to satisfy the course's learning outcomes by working with technology they are comfortable with. Despite the open-ended nature of the task, submitted assignments can be evaluated fairly quickly because students need to provide sufficient evidence they have planned, executed, and evaluated their exploits. As such, the presentation of this evidence evaluates both the effectiveness and appropriateness of their efforts.

Despite its benefits, there are three problematic aspects of this assessment task's design.

First, while the assignment engages students in the technical skills required to exploit computer systems, students fail to engage with the practices within which these are situated. These practices entail the application of both social and technical skills to establish the organisational context enabling a successful exploit. In theory, students can include this context as part of their write-up. In practice, students are only required to document the physical context necessary to replicate an exploit, and a reflective self-assessment of their results. While this self-reflection theoretically provides an opportunity for students to consider the different implications of their exploits, most Level I students have insufficient commercial experience to appreciate them.

Second, the assessment task fails to minimise opportunities for plagiarism. There are many "cookbooks" online for planning, conducting, and documenting exploits; these potentially allow students to pick pre-existing exploits and document these as their own. While this is not in-and-of itself a problem because it would beyond the means of the students to devise exploits of their own, the need to properly reference and compare & contrast their exploit with related work is considered neither in the task rubric nor the marking scheme.

Third, the feedback strategy entails providing feedback on the technical aspects of their exploits, and how they went about planning them. As such, if the students have problems understanding some of the technology they need to use, this may be hidden by their choice of exploits. This makes it difficult to provide feedback on underlying problems they may have with the related theory, which may not be discovered until they face their invigilated exam.

3.2 Revised Coursework Design

To build on the experiences and lessons learned from work such as [9] and [11], the coursework assignment for the 2013-2014 academic year was re-designed. Specifically, it was designed to employ realistic scenarios, and allow students to demonstrate a wider repertoire of cyber security practices than simply exploiting vulnerable machines.

Rather than being an open-ended task, the students were asked to evaluate the security of three different *targets* associated with a real-world case study. The evaluation of these targets was such that although an adversarial perspective needed to be taken, the outcome of the evaluation would be proposals that improve system security. The case study for the coursework assignment was the technology used to run a student bar; the bar in question was the topic of a recent Wired article [12]. By selecting a real organisation that students have some affinity with, and indicating that their assignments will help improve the security of the organisation, students would find the assignment engaging.

Based on lessons learned from [11], the coursework gave students an extended opportunity to re-apply skills developed in the class exercises. The coursework also built on the experiences of [9] by providing a real-world case study that

includes social and physical, as well as logical, security elements. The re-design also addressed two of the three problematic aspects of the previous assignment. It allowed students to demonstrate their application of cybersecurity practices, and ethical hacking in particular, rather than just applying generic exploits. In terms of feedback, the systems evaluated were the same for everyone, which simplified marking and moderation. It also made it harder for students to hide behind simple demonstrations of exploits, which hide difficulties digesting the course material. Although elements of self-reflection were built into the assignment, this focused on students making a case for the risks they identified during their evaluation, rather than evaluating what they have learned in general. However, as there was now a narrower range of skills and techniques for students to use, there were also increased opportunities for plagiarism.

When the revised coursework draft was subject to internal QA, concern was raised about what happens should students decide to overstep their ethical boundaries by "hacking" the college to complete the first part of the assignment. Fortunately, the assignment dealt with this concern in four different ways. First, in the overview of the first draft of the assignment, students were told they should not break the computer misuse act while completing the assignment. To reinforce this point, the statement was rephrased and emboldened to state students **must not break the Computer Misuse Act while completing the assignment**. Second, the rubric for Target 1 indicated that students needed to confirm the origin of any data they find to ensure it really is in the public domain. Because the assignment's author has expert knowledge of the case study domain (he was the Beer Manager for the Wolfson College Cellar Bar between 2008 and 2009), it would be easy to identify evidence not known to be in the public domain. Consequently, if students decided to overstep the mark and pass off their findings as publically available, this would be easy to identify. Third, the Wolfson College Bar Sub-Committee were aware of this assignment, and were asked to report back on any strange or unusual requests for information between January and April. Finally, the evaluation of Target 1 accounted for only 20% of the assignment's mark. As evaluating this target was largely independent of the other aspects of the assignment, students completing the assignment strategically were unlikely to break the law given the low return of doing so.

4.0 Critical Analysis of Coursework Design

While the revised coursework design appeared to be an improvement, it would benefit from a thorough evaluation before being released to students. This was particularly important given that many of the ideas upon which the revised coursework was based came from post-graduate, as opposed to undergraduate, education. To do this, the revised assignment was critically analysed. In the following sub-sections, the coursework was evaluated based on the following three criteria:

- Constructive Alignment: Does the coursework ensure the course's learning outcomes are satisfied?
- Engagement: Does the revised coursework engage the stakeholders associated with it?
- Plagiarism: Are opportunities for plagiarism minimised?

4.1 Constructive Alignment

Constructive Alignment is the principle of aligning teaching and assessment tasks using learning outcomes. In doing so, Constructive Alignment fuses a constructivist theory of learning, the alignment between Indicative Learning Outcomes (ILOs) of a course, the teaching activity, and the assessment task [13]. The ethical hacking course provides students ample opportunities for constructivism because probing and appropriate technology to find security vulnerabilities is intrinsically problem-based.

For the EHC course to demonstrate constructive alignment, appropriate learning outcomes are needed. Such learning outcomes are best expressed in general terms, and interpreted in light of the module context [3]. These learning outcomes, which are drawn from the course's unit specification, are as follows:

1. Elucidate the types of hackers and relate their activities to a legal framework.
2. Select and apply appropriate software tools to footprint, scan and enumerate digital resources.
3. Plan and conduct exploits associated with digital resources using a range of techniques.
4. Construct a security plan appropriate to a given application.

With the learning outcomes established, it is necessary to determine whether the assessment task demonstrates their satisfaction, and whether the learning activities enable the student to complete the assessment [14].

In considering the first criterion, the previous coursework assignment demonstrated satisfaction of the learning outcomes by primarily assessing ILO 3 and, to a lesser extent, ILO 2. The revised assignment assessment demonstrates not only the satisfaction of ILO 2 and 3, but also ILO 4. To help facilitate this, the revised assignment also indicates how different sections of the assignment -- the targets -- address these ILOs.

In considering the second criterion, as indicated in Section 3.2, the coursework ensured students re-applied skills and practices rehearsed during earlier classroom exercises. These included devising penetration test plans and proposing a penetration test report template (ILO 4), selecting and applying tools to find security vulnerabilities (ILO 2), and carrying out exploits to demonstrate their presence (ILO 3).

4.2 Student Engagement

Student engagement is the investment of time, effort, and other relevant resources by both students and their institutions towards an optimised student experience, enhanced learning outcomes, student development, and performance and benefit of the institution [15]. Although there are different perspectives and dimensions of engagement, which are described in detail by Trowler [16], underpinning these are two models: the market model and the development model [15]. The market model considers cybersecurity education as a market, where students are consumers, and the assignment task as a commodity. The assignment, and the skills and practices necessary to complete it, attract students to the Forensics & Computing programme, some of which consider the course as a "penetration-testing academy". The development model considers students as partners in cybersecurity education where, together with lectures and classes, the assignment is part of the development process delivering this.

To evaluate the revised assignment for student engagement, Trowler & Trowler's reflective questions were applied, and how the revised assignment attends to them was considered. In answering these questions, the revised assignment is considered to be the target of engagement, and the objects of engagement to be (i) engagement to improve course learning by meeting the learning objectives, and (ii) engagement to sensitise students with cybersecurity practices.

The first reflective question considers *Salience*: How important is the revised assignment compared to other initiatives on the students' programme, and professional practice? With respect to the programme, the assignment is an important vehicle for formative evaluation. The assignment allows students to not only reinforce skills developed during the labs, but also evaluate their own understanding of theory before their end-of-year examination. Where there is evidence of theoretical deficiencies, these can be highlighted in the assignment feedback. With respect to the practice, the assignment provides students with their first opportunity to carry out a realistic, albeit slightly contrived, security evaluation. As there is an external beneficiary, the assignment also provides experience they can market on their CVs while applying for industrial placements.

The second reflective question considers *Congruence*: How embedded is the revised assignment with current practices within the programme, and the professional practice the course prepares students for? With respect to the programme, the assignment is aligned with the unit specification, and previous class exercises prepared students for tackling the assignment. The assignment dates have been aligned with other course modules to ensure students are not working on multiple assignments at the same time. The assignment is made available during their first semester exam period to ensure it doesn't interfere with any teaching. With respect to the professional programme, the assignment allows students to apply complementary expertise to the ethical hacking skills used to evaluate the first target.

The third reflective question considers *Profitability*: How does the revised assignment benefit its academic and professional beneficiaries? The primary beneficiaries are students, who confirm their own knowledge in ethical hacking and related practices. There are two secondary beneficiaries. The first of these is the Forensics & Computing teaching team who obtain feedback on the capabilities of the students, and how to prepare them for their final year of teaching. The second is Wolfson College, who will receive feedback about vulnerabilities they may wish to address.

4.3 Plagiarism

As the coursework assignment is a non-invigilated activity accounting for half the students' final mark, plagiarism is an ever-present risk. Bloxham & Boyd [3] claim that the potential for plagiarism increases when assessments are repeated, are bunched at the end of courses, require only the use of information easily available in the public domain, and are not systematically checked. The novelty of the assignment, the need to analyse (as opposed to regurgitate) information in the public domain, and the need to produce an evidence base for their answers go some way towards removing these factors. To more thoroughly evaluate the revised assignment's potential for plagiarism, responses to the below checklist questions proposed by [3] are considered.

4.3.1. Regularly changing assessment questions

Because the coursework is a re-design from an open-ended question, to one based on a case study, there is no scope for plagiarism of the previous year's assignment. There is, however, scope for plagiarism in the 2014-2015 assignment if the same case study remains in use. There is also potential scope for plagiarism if the same type of organisation is used, and the type of targets evaluated remained the same. This is because academic institutions may share security vulnerabilities, and the approaches for exploiting targets may be identical or very similar.

4.3.2. Spreading assessment across the module

The dates for both releasing and submitting coursework to students was co-ordinated with other module leaders to ensure students were not working on multiple assignments for the same deadline. Moreover, arrangements were made to release the coursework during the examination period in the weeks before the start of the second semester. This ensures that, once their examinations are complete, students had no competing assessment tasks.

4.3.3. Developing own case study material based on contemporary events

As indicated in Section 3.2, the case study upon which the assignment is based was contemporary; the motivating article for the assignment was published only two months before the coursework was released.

4.3.4. Making assessments relevant and stimulating

Many students have experience of student bars during their studies and vacations. This experience provided students with a relevant context of investigation they would find stimulating.

4.3.5. Setting more specific titles for assessments

It was decided to give the same coursework assignment and brief to all students. Requiring students to propose their own coursework assignment would have been problematic for undergraduates starting their second year, and thus unable to appreciate the alignment between the course's learning outcomes, and the satisfying assessment tasks.

4.3.6. Using group assignments

When commercially employed, ethical hacking is a group rather than individual activity; this suggested a group assignment might be more appropriate than an individual one. However, because there is no group-based working element in the course's learning outcome, and the coursework aimed to evaluate technical skills individual students may not otherwise employ in a group, an individual assignment was deemed most appropriate.

4.3.7 Asking for copies of key sources to be appended to the coursework

In the assignment brief, students were told their results needed to be justified. Not only did the assumptions made need to be clearly stated, but also the origin of any data used to form the basis of their evaluation needed to be described. Moreover, where exploits were carried out, the steps taken to reproduce them needed to be included as an appendix to their submission.

5.0 Conclusion

Case studies reporting on the lessons learned teaching cybersecurity are increasing, yet there has been little emphasis on the role of assessment in cybersecurity pedagogy. This case study has helped fill this gap. In doing so, three contributions are made.

First, recent work in cybersecurity pedagogy is summarised. Based on this, useful themes to incorporate in ethical hacking assessment tasks were identified. While the related work is based on postgraduate education, many of these experiences are relevant. Nonetheless, this case study has shown that careful consideration is necessary for adapting these lessons given the less mature undergraduate students.

Second, an ethical hacking coursework assignment leveraging these themes was re-designed, which addresses weaknesses in the previous coursework template. At

first blush, the coursework appears to offer fewer opportunities for self-reflection. However, these opportunities do exist, but in a different guise; rather than asking students to reflect on their experiences from an adversarial perspective, they are instead asked to consider whether their recommendations improve the security of Wolfson College. Such contextualised self-reflection is typical of what students may be expected to carry out in practice as responsible penetration testers.

Finally, the re-designed assignment was critically analysed based on constructive alignment, student engagement, and plagiarism, and discussed how the re-designed assignment meets, or in some cases doesn't meet, these criteria. During an internal QA of the assignment, it was suggested that constructive alignment could be further improved by adding guidance about the form adequate and exceptional assignments might take. Unfortunately, as an emerging subject area, it is difficult to devise such guidance without making value judgements about tools and templates that students should use; this would be over-prescriptive given the pre-existing learning outcomes for the EHC course. This suggests that, in the long term, it may be necessary to devise learning outcomes that better fit the needs of Level I students. Revising these learning outcomes will be the subject of future work.

6.0 References

1 National Audit Office, "The UK cyber security strategy: Landscape review." February 2013.

2 Bournemouth University Market Research & Development, "BSc (Hons) Forensic Computing and Security Freshers Report." Autumn 2013.

3 S. Bloxham and P. Boyd, Developing Effective Assessment in Higher Education: A Practical Guide. Open University Press, 2007.

4 The Higher Education Academy, "HEA STEM (Computing): Cyber Security Pedagogy, Teaching and Learning in Higher Education 2013." http://www.heacademy.ac.uk/ events/detail/2013/29_May_Warwick-Computing, May 2013.

5 P. Y. Logan and A. Clarkson, "Teaching students to hack: Curriculum issues in information security," in Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, SIGCSE '05, (New York, NY, USA), pp. 157–161, ACM, 2005.

6 B. A. Pashel, "Teaching students to hack: Ethical implications in teaching students to hack at the university level," in Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, InfoSecCD '06, pp. 197–200, ACM, 2006.

7 S. Bratus, A. Shubina, and M. E. Locasto, "Teaching the principles of the hacker curriculum to undergraduates," in Proceedings of the 41st ACM Technical Symposium on Computer Science Education, SIGCSE '10, pp.

122–126, ACM, 2010.8 National Audit Office. The UK cyber security strategy: Landscape review. February 2013.
8 F. B. Schneider, “Cybersecurity education in universities,” Security Privacy, IEEE, vol. 11, no. 4, pp. 3–4, 2013.
9 T. Dimkov, W. Pieters, and P. Hartel, “Training students to steal: A practical assignment in computer security education,” in Proceedings of the 42Nd ACM Technical Symposium on Computer Science Education, SIGCSE ’11, pp. 21–26, ACM, 2011.
10 EC-Council, “Certified Ethical Hacking website.” https://www.eccouncil.org/Certification/certified-ethical-hacker, October 2013.
11 S. Standard, R. Greenlaw, A. Phillips, D. Stahl, and J. Schultz, “Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course,” ACM Inroads, vol. 4, pp. 52–64, Sept. 2013.
12 Wired, “Student hacks Raspberry Pi to run college bar.” http://www.wired.co.uk/news/ archive/2013-11/07/raspberry-pi-powered-bar, November 2013.
13 J. Biggs and C. Tang, Teaching for Quality Learning at University: What the Student Does. Society for Research into Higher Education & Open University Press, 4th ed., 2011.
14 The Higher Education Academy: Hospitality, Leisure, Sport and Tourism Network, “Topics in Learning and Teaching: Constructive Alignment.” http://www.heacademy.ac.uk/ hlst/resources/a-zdirectory/constructive_alignment, 2009.
15 P. Trowler and V. Trowler, Conceptual Overview of Student Engagement. Leadership Foundation for Higher Education, 2011.
16 V. Trowler, “Student engagement literature review,” The Higher Education Academy, 2010.