Does the BSc Computer Security and Forensics Course Develop the Skills Required by Employers in the Area of Penetration Testing?

Graham Winchester

01 November 2018

Contents

Introduction

What is the purpose of this paper?

This paper is going to look at the BSc Computer Security and Forensics Course offered and presented by The University of Bedfordshire. It is going to compare the skills gained by graduates of this course to the skills required by employers. It will also look at the skills required for the roll of a Penetration Tester and if BSc Computer Security and Forensics Course offers those to a graduate; leaving university and looking for employment in the field of Penetration Testing.

What is Penetration Testing?

Weidman (2014) sums up penetration testing as the following;

> *Penetration testing*, or *pentesting* (not to be confused with testing ballpoint or fountain pens), involves simulating real attacks to assess the risk associated with potential security breaches. On a pentest (as opposed to a vulnerability assessment), the testers not only discover vulnerabilities that could be used by attackers but also exploit vulnerabilities, where possible, to assess what attackers might gain after a successful exploitation.

In essence penetration testing is finding security vulnerabilities in a system before any attackers can cause any actual harm. Most of theses vulnerabilities or exploits could be avoided just by keeping systems up to date and making sure employees have up to date security training.

There are many stages to pen testing and these vary on the job. Most start with the *Pre-engagement*; Meeting the client and arranging the guidelines of the penetration test to take place. *Information-gathering*; Finding all publicly available information on the client and using this information to discover a way to gain access into their system. *Threat-modelling*; Checking the information gathered and the validity of that information to gaining access to the clients system. *Vulnerability Analysis*; Searching for vulnerabilities that can be exploited. *Exploitation*; Gaining access to the clients system using the vulnerabilities found. *Post-exploitation*; Using the information gathered to gain deeper access to the system and other connected systems. *Reporting*; Summarising all findings for the client and their technical team.

The Shortage of Well-qualified Graduates

Sullivan (2018) said “Amongst the many cybersecurity positions companies are currently challenged to fill are penetration testers’ roles” He also goes on to say “However, the problem isn’t a lack of qualified candidates; the problem is how companies approach penetration testing”. Research by Oltsik (2017) suggests that 23% of organizations report having a shortage of pen testers, ranking penetration testing fourth on the list of cybersecurity skills where they suffer the largest shortage.

Oltsik (2017) goes on to say that 69% of organizations planned to increase cybersecurity spending in 2017, 39% of organizations say that increasing cybersecurity protection is one of their highest business initiatives driving IT spending in 2017 and 32% of organizations say that strengthening cybersecurity tools and processes is one of their most important IT initiatives in 2017.

This data shows that cybersecurity is a massive part of an organizations info-structure and their needs for security will only increase as more organizations move to cloud based operations. According to Oltsik (2017) 17% of New IT initiatives such as cloud computing, mobile computing, etc. have been implemented without proper cybersecurity oversight and controls; causing the organization serious security events.

Skills gained on the BSc Computer Security and Forensics Course?

The BSc Computer Security and Forensics course offers according to (*Course information form: Computer security and forensics*, 2016); A focus on network security, systems hardening, the process of gathering evidence and analysing captured data, and the legal requirements for those who work in the area. They also go on to say; The course has been designed to develop graduates who are able to: Exhibit an advanced understanding of methods, concepts and technologies within the core area of Computer Security such as Incident Response, Security Testing, Forensic Investigation, Wireless Networks amongst others.

This course is split down into 12 units over 3 years. A student will complete 4 units each year, 2 units in the first semester and 2 units in the second. These units cover a range of topics from in the first year; Fundamentals of Computer Studies, Computer Systems Structures, Principles of Programming and Introduction to Software Development. With these units a student will build a foundation of skills and knowledge to be built upon in the second year. Learning; Networking, Operational Information Security Management, Security Testing, Forensic Investigation, Wireless Communications and networking.

What are Potential Employers of Penetration Tesers Looking for in Graduates?

Employers are looking for well skilled potential employees, preferably with multiple qualifications in their desired field. Along with applicable work experience in industry. Employers are also looking for employees with a variety of soft skills: excellent spoken and written communication, creative thinking, industry and market knowledge, team working abilities, leadership qualities and problem solving. Employers are looking for potential employees with professional development; individuals who are looking to gain more knowledge and skills. Be that though further education or voluntary work with different sectors and industries in their field.

In the field of penetration testing potential employers are looking for at least a relevant degree: computer science, cyber security, networking or forensic computing as a foundation with a few years experience in industry according to Bennett (2018). They will also be looking for potential employees with one or more certifications: GIAC Penetration Tester (GPEN), Offensive Security Certified Professional (OSCP) or Certified Ethical Hacker (CEH). These qualifications can be gained on the job or though self study, this is a combination of personal development and gaining industry experience.

Does the BSc Computer Security and Forensics Course Develop the Skills Required by Employers in the Area of Penetration Testing?

The BSc Security and Forensic course develops soft skills needed by employers and the relevant skills as an entry point into the field of penetration testing. But it does not give you the major skills to enter a position as a penetration tester as a graduate. A graduate will still have to employ personal development to gain the required certifications and qualifications, be that through further education or industry experience.

The BSc Computer Security and Forensics course will allow a graduate doing a practice year to get ahead with industry experience, but over-all they will still have to gain the needed qualifications required by employers. They will have the advantage over graduates not doing a practice year. Having actual industry experience will allow them to gain more industry experience as they will require less hands on training compared to a graduate with no industry experience. They will also gain needed soft skills from working in an actual business environment.

Conclusion

To conclude the BSc Computer Security and Forensics course offers more to a graduate taking a practice year than a graduate leaving and heading straight in to an industry position. This is more in experience and soft skills gained from working in a penetration testing position. A leaving graduate will have the applied skills, but will still need to build on self study and gain more certificates and experience.

References

Bennett, J. (2018) *Job profile: Penetration tester.* AGCAS. Available at: https://www.prospects.ac.uk/job-profiles/penetration-tester (Accessed: 1 November 2018).

Course information form: Computer security and forensics (2016). University of Bedfordshire. Available at: www.breo.beds.ac.uk (Accessed: 1 November 2018).

Oltsik, J. (2017) *The life and times of cybersecurity professionals.* United States: The Enterprise Strategy Group, pp. 1–41.

Sullivan, C. (2018) *Cybersecurity skills shortage: Where are all the penetration testers?* Infosecurity Group; Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/contacts/ (Accessed: 1 November 2018).

Weidman, G. (2014) *Penetration testing: A hands-on introduction to hacking.* 1st edn. San Francisco, California, United States: No Starch Press, pp. 1–528.

Assesment

Professionalism of report structure, presentation, spelling, grammar

Totally inappropriate standard of work – ie. informal, first person style	**E/F**
Inappropriate structure ie. missing introduction or headings. Many spelling errors poor sentence structure or use of commas.	**D**
Adequate structure and presentation but with significant flaws in spelling, grammar or style.	**C**
Good. Mostly appropriate but isolated minor flaws in structure, spelling and grammar.	**B**
Excellent. Appropriate structure with title, headings, introduction etc. Good sentence structure. Commas used appropriately.	**A**
—	—

Content and use of evidence

No supporting evidence provided – report based on personal opinion and assumption.	**E/F**
Content thin and could be more relevant or more up to date.	**D**
Adequate content. No attempt to evaluate or judge the claims being made.	**C**
Mostly well researched with evidence provided but some minor flaws in argument. Some attempt to critically evaluate or judge.	**B**
Well researched excellent - supporting evidence provided for claims. Good attempt at critically evaluating the claims described.	**A**
—	—

Referencing

No indication of sources.	**E/F**
Some attempt to indicate sources but major flaws with referencing.	**D**
Some attempt at indicating sources, but with significant flaws in referencing.	**C**
Good attempt at indicating sources with only minor flaws in referencing.	**B**
Fully referenced according to academic convention.	**A**
—	—

How have I improved my report as a result of the feedback I got on the draft version?

I cleared up some of the informal language, the length of sentences and paragraph structure.