Does the BSc Computer Security and Forensics course develop the skills required by employers in the area of Penetration Testing?

Graham Winchester

22 October 2018

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

(Weidman, 2014) sums up penetration testing quite simply;

> *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-modeling*; Checking the information gathered and the validity of that information to gaining access to the clients system. *Vulnerability Analysis*; Searching to vulnerabilities that can be exploited. *Exploitation*; Gaining access to the system. *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.

(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.

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 do 4 units each year, 2 for the first semester and 2 more in the second. These units cover a range of topic 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 and Forensic Investigation and Wireless Communications and networking.

References

Course information form: Computer security and forensics (2016). England: University of Bedfordshire, pp. 1–16.

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.