University of Essex | Online

Module Reflection

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Sunday 31st October 2021

Student ID: 126853

E-Portfolio Links:

GitHub Pages: https://eportfolio.kieronholmes.me/modules/network-information-security-management

Module Reflection:

The Network and Information Security Management module of the MSc Computer Science course provided us with an in-depth introduction to Information Security Management. Throughout the module, we have been introduced to the underlying technologies behind computer networks and common security concerns that should be considered when developing an e-Health site.

The first aim of this module required us to identify and analyse security risks and vulnerabilities in IT networks (UoEo, n.d.). During the Unit 6 seminar, we were introduced to an article by Geer (2015), including eight commonly used penetration testing tools, which can be used for host fingerprinting and vulnerability analysis. These tools were available by default on the Kali Linux variant, which was the operating system of choice for our summative assessment.

Following on from this aim, to complete the Unit 6 and Unit 11 assignments, we were required to investigate further and identify a series of vulnerability scanning tools used to identify issues with the e-Health site we had been assigned. Within our team, tools including Nikto, Nmap, Metasploit and OWASP ZAP were chosen due to their high prevalence within the penetration testing sector. This section has helped me understand the tools available to identify issues and the overall concepts, which will be used throughout any future development work I undertake.

The second aim of this module required us to design and appraise computer programs and systems (UoEo, n.d.). This aim required us to fully evaluate the systems and infrastructure chosen to host the site allocated to our team for investigation. Although the application was hosted on the Amazon Web Services (AWS) environment, it was clear that numerous security omissions would have prevented the site from being used for its intended purpose (e-Health).

Within the content for this aim, we had produced a document fully explaining the issues we had identified with the codebase of the assigned site. In addition, this document included details on what could have been done differently to reduce the number of vulnerabilities the site contained and steps that could have been implemented to aid legislative compliance. I will be using the knowledge learnt in this section throughout my day-to-day work and future modules.

The third aim of this module required us to gather information from appropriate online sources to aid the vulnerability assessment elements of this module. Within this section, we learnt the importance of using the OWASP Top 10 Web Application Security Risks (OWASP, n.d.), combined with the usage of the Common Vulnerability and Exposures (CVE) database hosted by Mitre (n.d.).

To test our knowledge and understanding of sourcing online vulnerability details, we were required to complete a comprehensive list of vulnerabilities (with sources) for the Unit 11 Executive Summary document. In addition, identified issues were linked to either an OWASP Top 10, Common Weakness Enumeration (CWE) or CVE item to provide a low-level overview and full technical details on how these can be prevented. This aim has helped me increase my understanding of the sources that can be used within a penetration testing scenario and where to find details on best practices and prevention.

The final aim of this module required us to articulate the legal, social, ethical and professional issues faced (UoEo, n.d.). Within this section, we learnt about appropriate legislation that would affect an IT professional working within the e-Health sector, namely the General Data Protection Regulations (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA). Throughout our group work, we were required to apply the concepts of this legislation to both the work we had undertaken and the selected business itself.

This section introduced us to the concepts and risks behind the modern Data Protection legislation and how it should be implemented to satisfy the requirements of the data subjects and the regulator(s). Within Unit 8, we were required to research a specific case study, identifying what could have been done differently to reduce the risk of the breach initially occurring. This section has helped me understand the legislative requirements and how to implement those in order to ensure data is kept secure and away from unauthorised users.

During the units included in this module, I had researched and participated in all of the discussions and assignments. Units throughout required the investigation of a series of Penetration Testing and diagnostic tools, such as Kali, Ping, Whois, Traceroute and NSLookup. Although this was a topic I was thoroughly aware of, it is not something I had previously been involved in documenting and presenting to a client. The methodologies recommended within this course, particularly STRIDE and

DREAD, will be used throughout my work to evaluate which vulnerabilities require more immediate action to preserve data/system integrity.

The Assignments due throughout this module required an element of group work. Therefore, as a group, we split each assignment into distinct tasks, which were then assigned to team members based on overall strengths/weaknesses. As our team had a few non-native English speakers, I found that occasionally there were a few issues with language differences, requiring sections of text to be re-written. Mellissa Welch-Ross (n.d.) states that knowledge of a second language commonly results in a series of structural differences being present in written work. Due to this, I would suggest that in future, work is conducted using a real-time collaborative writing tool such as Google Docs, combined with tools such as Grammarly to check the written content.

Throughout the module as a whole, I have completed various tasks to demonstrate my understanding of Computer Networks and Network Security. This has enhanced my knowledge of the Penetration Testing lifecycle and the tools and security methods that an organisation should implement within a cloud environment. The knowledge learnt from this module will be used within my current job and will be applied throughout the upcoming modules.

References:

Geer, D. (2015) 8 penetration testing tools that will do the job. Available from: https://www.networkworld.com/article/2944811/8-penetration-testing-tools-that-will-do-the-job.html [Accessed 31st October 2021].

Mitre. (n.d.) Frequently Asked Questions. Available from: https://cve.mitre.org/about/faqs.html [Accessed 31st October 2021].

OWASP. (n.d.) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 31st October 2021].

UoEo. (n.d.) Network and Information Security Management – Module Home. Available from: https://www.my-course.co.uk/course/view.php?id=7058&section=0 [Accessed 31st October 2021].

Welch-Ross, M. (n.d.) *Language Diversity, School Learning, and Closing Achievement Gaps*. Available from: https://www.nap.edu/read/12907/chapter/1 [Accessed 31st October 2021].