Network and Information Security Management – Units 4 - 6

This 12-week module introduces the various core elements of the MSc. Cybersecurity programme at the University of Essex Online. It intends to ensure a basic understanding of the primary skills covered in complete detail during all relevant modules. It also provides insight and understanding of how the different practices and occupational roles combine to offer a robust body of knowledge and skillset required to succeed in the field. Furthermore, it is beneficial to all who would master this critical field to gain a fuller understanding of the contribution and importance of all elements. As the units tend to build one upon another and contain summary review and reflection every few units, these note entries will follow a similar track and cover three units in each.

This unit summary covers units between 4 - 6, including the following outcomes:

- Perform basic troubleshooting and investigations using the tools provided as part of common operating systems (tools such as ping, traceroute and so on).
- Analyse the outputs provided by the tools.
- Discuss the difference between TCP/IP and the ISO/OSI protocol stacks.
- Describe the different network tools and components available.
- Explain when and where to use selected tools and components.
- Evaluate the security implications of using selected components.
- Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
- Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
- Articulate the legal, social, ethical and professional issues faced by information security professionals.
- Select a toolset to use for scanning and vulnerability testing.
- Justify your selection.
- Submit the first part of your course assessment.

Progressive Learning Experience

These units were more challenging and provided an opportunity to learn more about network fundamentals, a thorough review of various network components such as routers, firewalls, vulnerability scanning tools, and intrusion detection/prevention systems. Exploring network components have been an entirely new area and helped me to strengthen my network-focused understanding. Unit six was particularly interesting since it covered the initial stages of the team project. In addition to that, the diversity of viewpoints and experiences of other students provided the opportunity for growth. Collaborative learning discussions were a noticeable focus area across all units. These discussions were more challenging than traditional courses that rely on exams and promote critical thinking simultaneously. However, these interactions of collaborative learning discussions were an exciting exchange and provided invaluable insight and expanded methods of critical examination.

Personal Take-Away for Units 4 - 6

The first part of the project was about setting the scene to perform vulnerability scanning, including detection and testing. There were also several pre-requisites, such as appropriately selecting applicable standards (PCI-DSS) and regulations

(GDPR) after assigning business functions to the so-called website of the organisation. Debating on potential vulnerability scanning tools, interactions on the collaborative discussion forums regarding the outcome of these scanning and internal group discussions were particularly exciting. Moreover, it also solidified the required skills for purple team exercises.

Required Reading

The following reading assignments were available during these units:

- Russell, A.L. (2006) ‘Rough Consensus and Running Code’ and the Internet-OSI Standards War. *IEEE Annals of the History of Computing.*
- Russell, A. (2013) OSI: The Internet That Wasn’t (How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking)
- Niemietz, M. and Schwenk, J. (2015) *Owning Your Home Network: Router Security Revisited.*
- Geer, D. (2015) 8 Penetration Testing Tools That Will Do The Job. Network World
- Hubbard, D. (2009) The Failure Of Risk Management. 1st ed. Newark: John Wiley & Sons, Incorporated.
    - Chapter 5.
- Satria, D., Alanda, A., Erianda, A. and Prayama, D. (2020) Network Security Assessment Using Internal Network Penetration Testing Methodology.
- Gardner, D. (2011) The Open Group, SABSA Release White Paper on Aligning Enterprise, Security Architecture to Achieve Business Goals.
- Kaur, G., Kaur, N. (2017) Penetration Testing - Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science* 8 (3): 844-846.

Additional Reading

The following reading assignments were available during these units:

- a2hosting.com (2020) Instructions for using Ping, traceroute, etc.
- Schneier, B. (2004) *Secrets and Lies : Digital Security in a Networked World.* Indianapolis: Wiley.
    - Chapters 8 and 12
- Sinha, A. (2017) *Beginning ethical hacking with Python.* West Bengal: Apress.
    - Chapters 23 and 24
- Tang, A. (2014) A guide to penetration testing. *Network Security* 2014(8): 8-11
- Goralski, W. (2014) Learn About Differences in Addressing Between IPv4 and IPv6.
- Rosencrance, L., Kroon, D. & Gattine, K. (2019) OSI model (Open Systems Interconnection)
- Waitzman, D. (1990) A Standard for the Transmission of IP Datagrams on Avian Carriers.
- Raza, M. (2018) OSI Model: The 7 Layers of Network Architecture.
- Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview.* 8th ed. New York: IBM.
    - Chapters 1-5.

- Josang, A., Miralabe, L. and Dallot, L. (2015) Vulnerability by Design in Mobile Network Security. *Journal of Information Warfare* 14(4): 1-12.
- Johansson, J. (2016) Security Watch: The Most Misunderstood Windows Security Setting Of All Time.
- Benton, K. (2010) The Evolution of 802.11 Wireless Security.