Unit 2 Reflection

In this unit, we looked at the idea of classifying threats and vulnerabilities. The definitions of threats and vulnerabilities I found useful because they describe the essence of a cyber-attack: an unexpected security breach (threat) against an asset that is not secured correctly (vulnerability). To categories and assess the threat, we looked at Microsoft's STRIDE threat classification and DREAD risk rating models. I consider knowledge of STRIDE/DREAD together certifications such as Certified Information Systems Security Professional (Chapple et al., 2018), will better prepare me to reduce threat and vulnerabilities found within information systems. I research information about the Skills Framework for the Information Age (SFIA)—a collaboration between people with real practical experience in developing skills and competencies in a corporate environment— and how it provides additional skills to enhance understanding of information security. The framework lists several roles applicable to ISM, such as Information Security Technician, Infrastructure Specialist or Operations Support analyst.

This unit considered a hacking scenario that involved a medical mannequin (Glisson et al., 2015) to demonstrate how easily a medical dummy can be compromised using available tools. This scenario introduced Denial of Service (DoS) and brute force attacks that hackers leverage against information systems. DoS attacks attempt to overwhelm systems that aim to disrupt the system, while brute force attacks are employed against password policies in a system. Jang-Jaccard and Nepal (2014) list vulnerabilities as encompassing hardware, software, and network layers. Humayun et al. (2020) list further vulnerabilities as credential reuse, cross-size scripting (XSS), malware, phishing, man-in-the-middle attacks, and SQL injection. In their systemic mapping study, Humayun et al. (2020) consider DoS, malware and "other" as the top three vulnerabilities with DoS occupying 37% of vulnerabilities.

DoS vulnerability can be exploited by using a ping of death technique which sends Internet Control Message Packet (ICMP) network packets larger typically supported, for instance, ICMP packets that are over 100KB in size which may cause the machine to freeze, crash or reboot. Some tools that can be leveraged for DoS include Low Orbit Ion Cannon (https://sourceforge.net/projects/loic/) or OWASP Switchblade (https://owasp.org/projects/). Brute force attacks attempt to exploit weak password policies and are often leveraged in penetration testing. Tools in the category include Brutex (https://github.com/1N3/BruteX), AirCrack-ng (https://www.aircrack-ng.org/) used to assess WiFi network security or John the Ripper (https://www.openwall.com/john/), Rainbow Crack (http://project-rainbowcrack.com/) that uses pre-computed rainbow tables.

References

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5):973-993.

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015). Compromising a medical mannequin. arXiv:1509.00065.

Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45(4):3171-3189.

Chapple, M., Stewart, J.M. & Gibson, D. (2018). CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.

SFIA (2021). SFIA 8 – the new version of SFIA is now live. Available from https://sfia-online.org/en [Accessed 3 Dec. 2021]

Bibliography

Tundis, A., Mazurczyk, W. and Mühlhäuser, M. (2018). A review of network vulnerabilities scanning tools: types, capabilities and functioning. *Proceedings of the 13th International Conference on Availability, Reliability and Security:*1-10.

Wang, Y. & Yang, J. (2017). Ethical hacking and network defense: choose your best network vulnerability scanning tool. I31st International Conference on Advanced Information Networking and Applications Workshops (WAINA):110-113.