E-Portfolio link **https://jhines2022.github.io/eportfolio/module%203.html**

Reflective Review

Word Count: 795

Unit 1

Undertaking the “security implications of the digital economy” discussion led me to having many questions and ended with an improved understanding of the different challenges between different business models.

One thought provoking moment was when Spremić & Šimunic (2018) stated ‘the main focus of cybersecurity is to design and implement effective controls', this made me question blue and red teaming roles. Defensively, implementing controls to enforce the CIA triad, but, is the true meaning of red teaming to test if those controls have been implemented or to test if product developers have created a product with “Secure by design” in mind. I also wondered how small businesses handled the effective controls implementation considering the “Competence” challenges around hiring and “technical ability”.

Being a visual learner, the Lockheed Martin cyber kill chain as illustrated by Hutchins et al, (2011) had given me a visual overview to aid my type of learning and provided an anchor point for further learning of the lecturecast and therefore, allowed me to apply the thinking in my CLD1 “initial post”.

Unit 2

Following on from the previous unit, this task pivoted around the Cyber Kill Chain and taught me how to look at an incident from a high level perspective, which, according to Orchilles (2022), is designed for conveying situations to non-practitioners. I learned how to apply a simple analysis and build a recommended mitigation theory based on the structured phases within the cyber kill chain template, as presented by Hutchins et al, (2011). Additional reading then clarified the progression and development of the MITRE ATT&CK in 2015 (Orchilles, 2022) and further development of the “Unified Cyber Kill Chain” in 2017 to extend collective exploratory power in modern attacks (Pols, 2017).

Unit 3

This unit was a huge challenge but a great learning experience. In preparation for tasks in this module, I carried out additional steps as illustrated in figure.1 due to wanting to explore a vulnerability plan, in the linux environment.

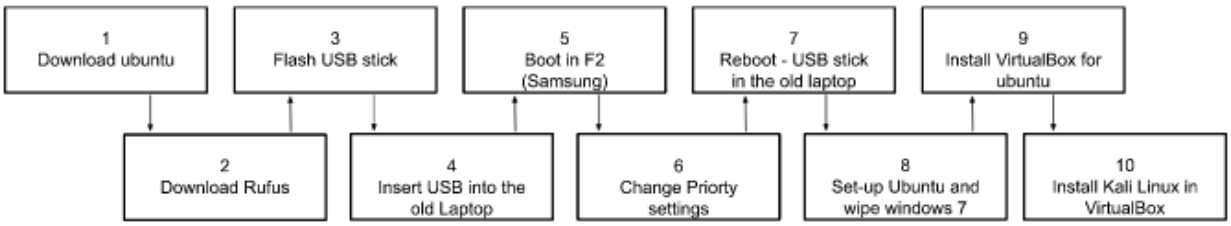

Figure.1 - Steps taken during the successful installs

Using the new linux terminal, the scanning activity helped with visualizing what information could be gained and planned for in the vulnerability report task, implementing simple commands via the terminal such as “Traceroute” and “MTR” for the scanning activity.

I was introduced to scanning policies, associated risks, tools and the different approaches of presenting to stakeholders which I think is very important because clear communication to ensure compliance and understanding is important.

I made many mistakes in this unit with the system preparation, experienced almost 3 days of continuous failure via trial and error until I eventually installed the correct compatible versions by mapping out each step taken.

Unit 4

This breach analysis taught me alot about the legal implications and how cross border laws can challenge national regulations.

The Aadhaar breach analysis case study highlighted many legal and cross border challenges. Firstly, GDPR is the toughest privacy and security law in the world (GDPR.EU, 2020) but only applies to Aadhaar if the company encroaches into the EU and not on EU citizens in India. I also discovered that the Aadhaar Act means: non-citizens who spend more than 182 days in India within a 12 month period must also register their details (Ministry of Law and justice, 2022).

My thoughts on this is: how do we enforce device and data privacy for employees and businesses who travel in and out of various jurisdictions while adhering to all rules and regulations?

Unit 5

My new understanding of logging, the importance of using LogRotate and the options of combining Nagios and Snort while implementing a SIEM have made conversations in the workplace easier and of benefit. One conversation evolved around cloud, potential issues for forensics investigations and auditing and how it could possibly have implications for compliance, regulations and legal investigations.

While researching vulnerability scanning in this unit, I discovered the Software Composition Analysis (SCA) tool that can passively scan open-source software (Enisa 2023:26) and create an SBOM for inspections at a later date (Enisa 2023:34) which will become valuable knowledge.

Unit 6

The vulnerability executive summary report had been a challenge to present the findings in a non-technical way due to the nature of the report. I have learned alot about exploits, software version control and mitigation from cross referencing vulnerabilities with CWE/CVE.

Conclusion

Although vulnerability analysis had been a large part of this module, I feel that the additional tasks and reading had also provided a solid baseline with a wide arch of key information which connects together. As a result of the tasks within this module, I have become a stronger asset to my company, my colleagues and grown in confidence to interact on more topics around logging, compliance and passive vulnerability scanning.

References

Enisa (2023) Developing national vulnerability programmes. Available at: https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes. [Accessed on 23rd February 2023]

GDPR.EU (2020) General Data Protection Regulation. Available from: https://gdpr.eu/tag/gdpr/ [Accessed 15th February 2023].

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in
Information Warfare & Security Research, 1(1), 80.

Ministry of Law and Justice (2022) Aadhaar Act 2016. Available from: https://www.indiacode.nic.in/ [Accessed 15th February 2023].

Orchilles, J (2022) Cyber Kill Chain, MITRE ATT&CK, and Purple Team. SANS Available at: https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/ [Accessed on 19th January 2023]

Pols, P (2017) The Unified Kill Chain - *Raising resilience against advanced cyber attacks*. Available at: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf [Accessed on 19th January 2023]

Spremić, M. and Šimunic, A., 2018, July. Cyber security challenges in the digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers