Vulnerability Analysis – Literature Review Activity

Reflect on this activity by answering the following questions:

1. Did you have any issues or challenges with the literature search/audit on software sites and the national vulnerabilities database?
2. How did you overcome them?
3. How will they affect your final report?

1. **Did you have any issues or challenges with the literature search/audit on software sites and the national vulnerabilities database?**

The issues with the literature review were:

- Ensuring that the literature was up-to-date and relevant
- Moving from the theoretical concepts to the technical implementation

The cyber security landscape is changing at pace. Some of the literature represents conceptual challenges and outlines foundational principals of cyber security. In those circumstances, the literature is helpful, relevant and informative. There is a time lag between academic research and current developments that may not always be helpful. The assigned website for this study is a social media platform and there are many threats that would be topical, current and relevant to a real-life activity but are not covered by academic literature at present. For example, Apple's current response to the UK government regarding end-to-end encryption would be topical, alongside Meta's stance on WhatsApp security. While these represent corporate viewpoints in relation to the tension between communication privacy (personal security) and government intervention (state security). There is scant academic research into this area.

Furthermore, the were challenges when reviewing more technical documentation, signposted from the course reading. For example, to gain a depth of understanding of the tools it is necessary to engage with them. This can be challenging when the recommended reading results in technical dead ends due to incorrect links or installation instructions.

2. **How did you overcome them?**

The challenges regarding up-to-date academic information meant that while wider reading and an awareness of news and topical issues is helpful, it is important to rely on academic sources to draw conclusions and separate them form opinions.

The technical links, downloads were overcome with resilience and allocation of additional time beyond what may be seen as reasonable.

3. **How will they affect your final report?**

The impact on the final report, is such that there may be a lack of depth from the technical response and the overarching resources have necessarily focused on the theoretical aspects in such a short period of time.

The changing landscape of cyber-security would affect the final report in that while the exercise mirrors a real-world scenario, if may be limited if it were to be implemented in action.

References

Alshamrani, A. et al. (2019) 'A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities', *IEEE Communications Surveys & Tutorials*, 21(2), pp.1851-1877.

Bennouk, K. et al. (2024) 'A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies', *Journal of Cybersecurity and Privacy*, 4(4), pp.853-908.

Dewhurst, R. (2013). *Static Code Analysis* | *OWASP*. Available at: https://owasp.org/www-community/controls/Static_Code_Analysis [Accessed 08 February 2025]

ICO (2024). UK GDPR guidance and resources. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ [Accessed 08 February 2025]

Kaufman, C. et al. (2022) *Network Security: Private Communications in a Public World.* Addison-Wesley Professional

Lachkov, P., Tawalbeh, L.A. and Bhatt, S. (2022) 'Vulnerability assessment for applications security through penetration simulation and testing', *Journal of Web Engineering*, 21(7), pp. 2187-2208.

McNab, C. (2017). *Network Security Assessment: Know your Network*. 3rd ed. Beijing: O'Reilly Media

National Cyber Security Centre (2023). *Cyber Essentials: Requirements for IT infrastructure v3.1.* Available at: Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf [Accessed 08 February 2025]

OSWAP (2021). *Top 10 Web Application Security Risks*. Available from: OWASP Top Ten | OWASP Foundation [Accessed 08 February 2025].

Sinha, S. (2017). *Beginning ethical hacking with Python*. West Bengal: Apress

Spraul, V.A. (2015). *How Software Works: The Magic Behind Encryption, CGI, Search Engines, and Other Everyday Technologies*. San Francisco: No Starch Press.

Uya, F. (2024). *Cybersecurity and Social Media: Does TikTok Pose Cybersecurity Risk to the United States?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4784942 [Accessed 08 February 2025]