Unit 4: Breach Analysis and Mitigation

The reading this week focusses on the issues around security breaches. Schwartz and Janger (2007) discuss the legal implications of security breaches. The articles below discuss the use of Kali Linux (and its associated tools) and provide a number of recommendations about their use. Bhatt (2018) sections 4 and 5 provide an overview of some of the most commonly used tools in Kali Linux and how to access them.

Required Reading

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

- Chapters 1, 2, 6 and 7

Bhatt, D. (2018) *Modern Day Penetration Testing Distribution Open Source Platform*. Kali Linux Study Paper.

Bhingardeve, N. & Franklin, S. (2018) *A Comparison Study of Open Source Penetration Testing Tools*.

Ekelhart, A. et al (2018) Taming the logs - Vocabularies for semantic security analysis. *Procedia Computer Science* (137).

Hill, M. & Swinhoe, D. (2021) *The 15 biggest data breaches of the 21st century*.

Additional Reading

Kaur, G. (2017) Penetration Testing – Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science* (3).

Schwartz, P. & Janger, E. (2007) *Notification of Data Security Breaches*. Michigan Law Review.

The Guardian (2016) The Five Steps of Incident Response*.*

It's Foss (2020) *The Kali Linux Review You Must Read Before You Start Using It.*

Dynatrace (2021) The Log4j vulnerability explained: What is Log4Shell?