Unit 5: Logging, Forensics and Future Trends

The reading this week focusses on on techniques for deploying and configuring logging and auditing solutions. Hertzog et al (2017) gives a good overview of Kali Linux and its operating modes (i.e., whether to run it from USB, DVD or to install it – we would recommend either of the first two). You are also provided with a vulnerability assessment report template, created by PurpleSec, which is required for the activity in this Unit.

Required Reading

Hertzog, R. et al (2017) Kali Linux Revealed (KLR/PEN-103) - *Mastering the Penetest Distribution*.

SANS Institute (2010) *Successful SIEM and Log Management Strategies for Audit and Compliance*.

PurpleSec (n.d) Sample Vulnerability Assessment Report - Example Institute.

Additional Reading

Vielberth, M. (2018) *A Security Information and Event Management Pattern*.

Grispos, G. (2017) *Security Incident Recognition and Reporting (SIRR): An Industrial Perspective*.

SolarWinds *Windows Logging Basics - The Ultimate Guide To Logging*.

Network Functions Virtualisation - Introductory White Paper.

Parziale, L. et al (2006) *TCP/IP Tutorial And Technical Overview*.

- Chapters 23-24