Resources on Intrusion Detection Systems: Core Elements

Preparation Lecture 7

- Refresh probability theory by studying probability and conditionals in Chapter 2:
  Introduction to Mathematical Statistics by D. Wackerly et al.
  https://tinyurl.com/59593y28
  You can expand to discrete/continuous distributions on Chapters 3, 4, and refresh the theory of the normal distribution.

- Read in detail the base-rate fallacy in the context of IDS:
  The base-rate fallacy and the difficulty of intrusion detection, S. Axelsson
  Emphasize on sections 3, 4, 5. Section 3 describes desirable properties of an IDS. Section 4 describes the Bayes rules needed and section 5 applies these rules on an IDS. https://dl.acm.org/doi/pdf/10.1145/357830.357849

Literature Lecture 7

- Understanding the ROC curve:
  An introduction to ROC analysis, T. Fawcett
  https://people.inf.elte.hu/kiss/13dwhdm/roc.pdf
  Emphasize on sections 1, 2, 3, section 5 algorithm 1 and section 7. For a simplified version you can also look at *Better decisions through science, J. Swets et al.*
  https://www.math.ucdavis.edu/~saito/data/roc/swets-dawes-monahan-ROC.pdf

- General information about IDS:
  Chapter 9 from Network Security Essentials and Standards, Stallings
  https://tinyurl.com/5xkcdvca