Curriculum: KEA System Security F2022 course

Below are the required reading for the course KEA System Security F2022.

Maybe compare to the exam subjects list, and keywords.

Primary literature

Primary literature - not all chapters are part of the curriculum:

- *Computer Security: Art and Science*, 2nd edition 2019! Matt Bishop ISBN: 9780321712332 1440 pages
- *Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin ISBN: 978-1-491-96038-7 284 pages
- *Forensics Discovery*, Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages. Can be found at http://www.porcupine.org/forensics/forensic-discovery/ but recommend buying it. Referenced below as FD

The following chapters are curriculum:

- *Computer Security: Art and Science*: chapters 1,2,4,6,7,8, 10, 11 until and including 11.4, 12 until and including 12.5.3.10, 13 until and including 13.5, 14-16, 18, 23, 25, 26, 27
  Note: skip/skim some policy language examples, skip 4.7, skip 5.2.3 and similar math parts throughout the book!
  Skim read if you can: chapters 5, 24, 28, 29, 30 appendix G
- *Defensive Security Handbook*: chapters 1-8, 19-20
  Skim read if you can: chapters 10-12
- *Forensics Discovery*, basic concepts of computer forensics must be known, the book as a whole is not curriculum, skim reading chapters 1-6, and appendix B are highly recommended

The following documents are curriculum:

- Smashing The Stack For Fun And Profit, Aleph One
  `stack_smashing.pdf`
- NCSC IT Security Guidelines for Transport Layer Security
  `IT+Security+Guidelines+for+Transport+Layer+Security+v2.1.pdf`
- TCP Synfloods - an old yet current problem, BSDCan slides
  `http://quigon.bsws.de/papers/2017/bsdcan/`

Curriculum: KEA System Security F2022 course

- Campus Operations Best Current Practices, NSRC
  `Campus_Operations_BCP.pdf`
- Mutually Agreed Norms for Routing Security (MANRS)
  `MANRS_PDF_Sep2016.pdf`
- Blog post about Mitre ATT&CK
  `Mitre-ATTACK-101-Medium.pdf`

The following concepts are to be known, as concepts at least, read introduction and table of contents:

- CIS controls, Center of Internet Security
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Special Publication 800-63B, concept here are also NIST Special Publications in general
- Enterprise Survival Guide for Ransomware Attacks, Shafqat Mehmoon, SANS Reading room
- Incident Handler's Handbook, Patrick Kral, SANS Reading room
- Download and browse the ENISA papers listed under Computer Forensics in the reading list, ENISA as a concept is also required