Communication and Network Security 2022 course

Below are the required reading for the course KEA Communication and Network Security 2022

Maybe compare to the exam subjects list, and keywords.

Primary literature

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

- *Applied Network Security Monitoring Collection, Detection, and Analysis*, 2014 Chris Sanders
  ISBN: 9780124172081 - shortened ANSM
- *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems*, 3rd edition 2017,
  Chris Sanders ISBN: 9781593278021 - shortened PPA
- *Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali*. OccupyTheWeb, December 2018, 248 pp.
  ISBN-13: 978-1-59327-855-7 - shortened LBfH

The following chapters are curriculum:

- *ANSM*: chapters 1,2,3,4, 7,8,9,10,13,14,15
  Skim if you like: chapter 11, 12
- *PPA*: chapters 1,2,3,4,5,6,7,8,9,10,11,12,13 – the whole book

The following documents are curriculum:

- NCSC IT Security Guidelines for Transport Layer Security
  IT+Security+Guidelines+for+Transport+Layer+Security+v2.1.pdf
- Mutually Agreed Norms for Routing Security (MANRS)
  MANRS_PDF_Sep2016.pdf

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

- *LBfH*: as needed to run commands, we have used multiple interesting programs: sslscan, nmap etc. you are free to bring these into play
  during exam
- Virtual Private Network https://en.wikipedia.org/wiki/Virtual_private_network

- WPA Cracking: Tutorial: How to Crack WPA/WPA2 `http://aircrack-ng.org/doku.php?id=cracking_wpa`

- `https://en.wikipedia.org/wiki/Sender_Policy_Framework` `https://en.wikipedia.org/wiki/DMARC` `https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`

- Campus Operations Best Current Practices, NSRC
  `Campus_Operations_BCP.pdf`

- Skim: `https://nsrc.org/workshops/2015/sanog25-nmm-tutorial/materials/snmp.pdf`

- Zeek documentation Intel framework `https://docs.zeek.org/en/stable/frameworks/intel.html` Suricata reputation support `https://suricata.readthedocs.io/en/latest/reputation/index.html`

- Skim: table of contents of RFC5246 The TLS Protocol Version 1.2, `https://www.rfc-editor.org/rfc/rfc5246.html` and the wikipedia page `https://en.wikipedia.org/wiki/Transport_Layer_Security`

- Skim: table of contents of RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks, `https://www.rfc-editor.org/rfc/rfc2827.html`

- Firewalls and filtering, perhaps take a look at my book in Fronter, *book-firewalls-and-packet-fitering.pdf*