NETVÆRKS- OG KOMMUNIKATIONSSIKKERHED

Introduktion

daka@kea.dk | coag@kea.dk

Agenda

- Gensidig introduktion
- Forventningsafstemning
- Formalia
  - Emner og plan
  - Eksamensform
  - Afleveringer
- TCP/IP modellen
- Challenge
- Software installation

Præsentation

- Dany Kallas
- Married, 2 kids
- DTU, IHK and ITU
  - Certified Web penetration tester and ethical hacker (GWAPT)
- Network engineer, Software developer

Præsentation

- Constantin Alexandru Gheorghiasa (**Alex**)
- Married, 0 kids
- KEA, ITU
- Software developer, Teaching

KØBENHAVNS ERHVERVSAKADEMI

IT University of Copenhagen

KØBENHAVNS ERHVERVSAKADEMI

Praktikaliteter

- Undervisning:
  - 21/9, 28/9, 12/10, 19/10, 26/10, 2/11, 9/11, 16/11, 23/11, 30/11, 7/12, 14/12
  - Alle dage 16.00-20.30
- Foreløbig tidsplan på fronter
- Besøg og oplæg fra eksterne vil blive opdateret I kalenderen

Eksamen

- D. 20 december 2017
- Test på paratviden omkring pensum stof
- Trækker 2 spørgsmål til eksaminationen (ingen forberedelsestid)
- 30 minutter inkl. karaktergivning (typisk eksamination på 20-25 minutter)

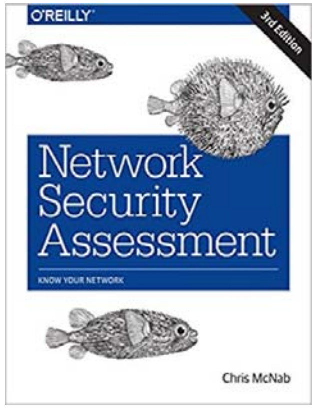
Kursus materiale

Network Security Assessment: Know Your Network

by Chris McNab

ISBN-10: 1491910955

ISBN-13: 978-1491910955

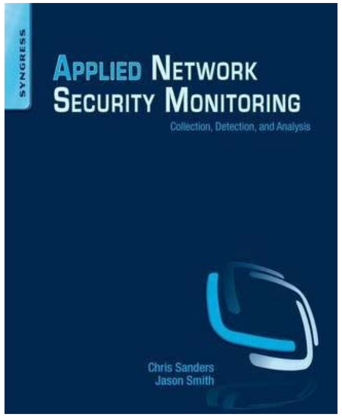


Applied Network Security Monitoring : Collection, Detection, and Analysis

by Chris Sanders

ISBN-10: 124172083

ISBN-13: 978-0124172081


SYNGRESS
Applied Network Security Monitoring
Collection, Detection, and Analysis
Chris Sanders
Jason Smith

Kursus materiale (ekstra)

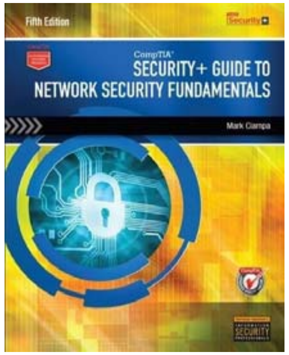
CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) 5th Edition

by Mark Ciampa (Author)

ISBN-10: 1305093917

ISBN-13: 978-1305093911

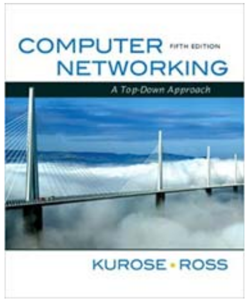
OBS! Dyr bog.
God at have men ikke strengt nødvendig!

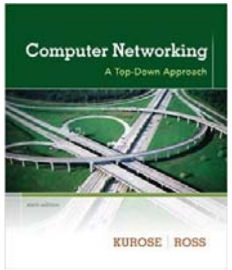


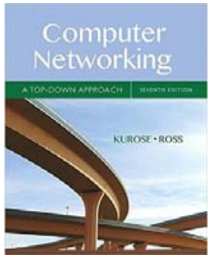
Computer Networking: A Top-Down Approach (any edition above 2nd is fine)

By Keith W Ross & James F Kurose

Billederne her er fra forskellige udgaver







Forventninger

- Brug de næste 5-10 minutter på at lave en prioriteret liste over de top 5 emner du synes burde være en del af kurset.
- Tal gerne med din sidemand.

Emner

- Security in TCP/IP
- Packet capture and Netflow
- Network segmentation, IDS/IPS
- Firewalls and Logfile analysis
- Network management
- VPN PPTP/IPSec/OpenVPN
- Application layer attacks, example Brokken HTTPS (Heartblead)
- Wifi Security

Crash course on TCP/IP model

- What is the layered model?
- Why do we have layers?
- OSI vs TCP/IP?
- Most important protocols

Network Challenge

Network attacks

- Attacks against the end system applications
- Attacks against infrastructure
  - Attacking the TCP, IP, ICMP
  - Attacking the network devices
- Getting behind core defences

Stages of an attack (The Cyber Kill Chain)

Reconnaissance

Weaponization

Delivery

Installation

C&C

Accomplish the task

Goal

DOS

Hijacking

Penetration/leaking

Installing software

- Download and install VMware Workstation
  - http://onthehub.com/download/software-discounts/vmware
- Download kali linux (32 or 64 depending on your system)
  - https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
- MAMP, XAMP, WAMP or LAMP
  - https://www.mamp.info/en/downloads/
  - http://www.wampserver.com/en/
- Download and install Wireshark (and WinPCap when asked)
  - https://www.wireshark.org/download.html