





Welcome to

# KEA Competence Diploma in IT-security

Henrik Kramselund Jereminsen [hkj@zencurity.com](mailto:hkj@zencurity.com) @kramse  

Slides are available as PDF, [kramse@Github](mailto:kramse@Github)  
0-diploma.tex in the repo security-courses

## High level description



### Diplom i it-sikkerhed, english: Diploma of IT-Security.

Sorry, danish only

**Diplomuddannelsen i IT-Sikkerhed** er en **erhvervsrettet videregående uddannelse** målrettet ansatte i virksomheder og organisationer med en væsentlig anvendelse af it.

Uddannelsen er udviklet i samarbejde med brancheorganisationer og erhvervsliv for at imødekomme et stort og stigende behov for **medarbejdere med specialiseret viden om it-sikkerhed**.

Diplomuddannelsen i IT-Sikkerhed er en **deltidsuddannelse**, der løbende tilpasses udviklingen inden for it- og cybersikkerhed.

Indholdet i de enkelte fagmoduler vil løbende blive opdateret til at møde de it-udfordringer, som virksomhederne står overfor.

Source: <https://kompetence.kea.dk/uddannelser/it/diplom-i-it-sikkerhed>

# Access Requirements



## Adgangskrav

For at blive optaget på Diplomuuddannelsen i it-sikkerhed skal du have en af følgende uddannelser:

- En relevant uddannelse mindst på niveau med en erhvervsakademiuddannelse, fx datamatiker, it-teknolog eller tilsvarende
- En relevant akademiuddannelse

Desuden skal du have mindst 2 års erhvervserfaring efter din adgangsgivende uddannelse. Opfylder du ikke de nævnte krav men har andre tilsvarende kompetencer, kan den enkelte institution dispensere efter en individuel kompetencevurdering. Kontakt uddannelsesinstitutionen for yderligere herom.

realkompetencevurdering – *what you know already*

<https://kompetence.kea.dk/uddannelser/studievejledning/realkompetencevurdering>

# Overview Diploma in IT-security - 60 ECTS total



Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Systemsikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Softwaresikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

## Course Data, example



### **Course: Computer Systems Security VF 3 Systemsikkerhed (10 ECTS)**

Teaching dates: tuesdays and thursdays 17:00 - 20:30

28/01 2020, 30/01 2020, 04/02 2020, 06/02 2020, 11/02 2020, 13/02 2020, 18/02 2020, 20/02 2020, 25/02 2020,  
27/02 2020, 03/03 2020, 05/03 2020, 10/03 2020, 12/03 2020

Exam: 31/03 2020

# Deliverables and Exam



- Exam
- Individual: Oral based on curriculum
- Graded (7 scale)
- Draw a question with no preparation. Question covers a topic
- Try to discuss the topic, and use practical examples
- Exam is 30 minutes in total, including pulling the question and grading
- Count on being able to present talk for about 10 minutes
- Prepare material (keywords, examples, exercises) for different topics so that you can use it to help you at the exam
- Deliverables:
- 2 Mandatory assignments
- Both mandatory assignments are required in order to be entitled to the exam.

# Course Description, example System Security



From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018

Indhold: Den studerende kan udføre, udvælge, anvende, og implementere praktiske tiltag til sikring af firmaets udstyr og har viden og færdigheder der supportere dette.

## Viden

Den studerende har viden om:

- Generelle governance principper / sikkerhedsprocedurer
- Væsentlige forensic processer
- Relevante it-trusler
- Relevante sikkerhedsprincipper til systemsikkerhed
- OS roller ift. sikkerhedsovervejelser
- Sikkerhedsadministration i DBMS.



## Færdigheder

Den studerende kan:

- Udnytte modforanstaltninger til sikring af systemer
- Følge et benchmark til at sikre opsætning af enhederne
- Implementere systematisk logning og monitorering af enheder
- Analysere logs for incidents og følge et revisionsspor
- Kan genoprette systemer efter en hændelse.





## Kompetencer

Den studerende kan:

- håndtere enheder på command line-niveau
- håndtere værktøjer til at identificere og fjerne/afbøde forskellige typer af endpoint trusler
- håndtere udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke it-sikkerhedsmæssige hændelser
- håndtere relevante krypteringstiltag

Final word is the Studieordning which can be downloaded from

<https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed>

Studieordning\_for\_Diplomuddannelsen\_i\_IT-sikkerhed\_Aug\_2018.pdf

# Course Materials



This material is in multiple parts:

- Slide shows - presentation - this file
- Exercises - PDF which is updated along the way

Additional resources from the internet

Note: the presentation slides are not a substitute for reading the books, papers and doing exercises, many details are not shown

My materials are open source:

- <https://github.com/kramse/security-courses>
- <https://zencurity.gitbook.io/kea-it-sikkerhed/>

# Primary literature – System Security



Primary literature - not all chapters are curriculumr:



Free graphics by Lumen Design Studio

- *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

Supporting literature:

- *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
- *Kali Linux Revealed Mastering the Penetration Testing Distribution* Raphael Hertzog, Jim O'Gorman - shortened KLR

# Primary literature – Communication and Network Security



Primary literature are these three books:

- *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

# Primary literature – Software Security



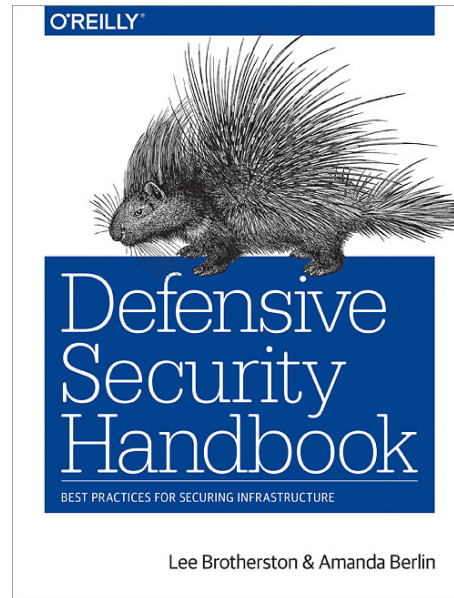
Primary literature:

- *The Art of Software Security Testing Identifying Software Security Flaws*, named AoST or the Green Book Chris Wysopal ISBN: 9780321304865, AoST or the Green Book
- *Web Application Security*, Andrew Hoffman, 2020, ISBN: 9781492053118 called WAS
- *Hacking, 2nd Edition: The Art of Exploitation*, Jon Erickson, February 2008, ISBN-13: 9781593271442, called just hacking



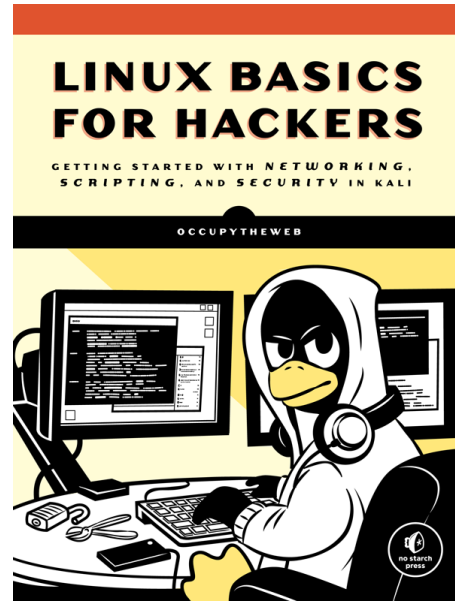
Free graphics by Lumen Design Studio

# Book: Defensive Security Handbook (DSH)



*Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin ISBN: 978-1-491-96038-7

# Book: Linux Basics for Hackers (LBfH)



*Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali* by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

<https://nostarch.com/linuxbasicsforhackers> Not curriculum but explains how to use Linux