Welcome to

# 0. Introduction

## KEA Kompetence Computer Systems Security 2020

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse 🐦

Slides are available as PDF, kramse@Github

0-Introduction-system-security.tex in the repo security-courses

# Contact information



- Henrik Kramselund Jereminsen, internet samurai mostly networks and infosec
- Independent network and security consultant
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hlk@zencurity.dk      Mobile: +45 2026 6000

You are welcome to drop me an email

# Plan for today

- Create a good starting point for learning
- Introduce lecturer and students
- Expectations for this course
- Literature list walkthrough
- Prepare tools for the exercises
- Kali and Debian Linux introduction

Exercises

- Kali Linux installation
- Debian Linux installation

Linux is a toolbox we will use and participants will use virtual machines

# 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

Note: parts of this material are quotes from the book we use, and similar courses. See the README in the Github reposity in the repo security-courses for this course 0-Introduction-system-security kramse@Github

A special thanks to William D. (Bill) Young Associate Professor of Instruction and Research Scientist, The University of Texas at Austin

When asked if I could borrow parts from his CS361 *Introduction to Computer Security* he graciously wrote:
"You are welcome to use them freely. You can credit me at the beginning."

# Fronter Platform
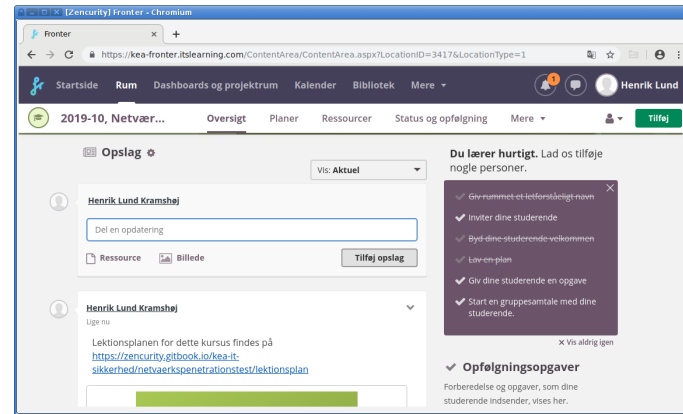


We will use fronter a lot, both for sharing educational materials and news during the course.

You will also be asked to turn in deliverables through fronter

`https://kea-fronter.itslearning.com/`

If you haven't received login yet, let us know

# Overview Diploma in IT-security

| |
|---|
| 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

## 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, wireshark captures) 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

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

**Færdigheder**

Den studerende kan:

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

# Kompetencer

**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`

# Expectations alignment



Form groups of 2-3 students

In groups of 2 students, brainstorm for 5 minutes on what topics you would like to have in this course

Use 5 minutes more on Agreeing on 5 topics and prioritize these 5 topics

PS We will from time to time have exercises, groups dont need to be the same each time.

# Primary literature

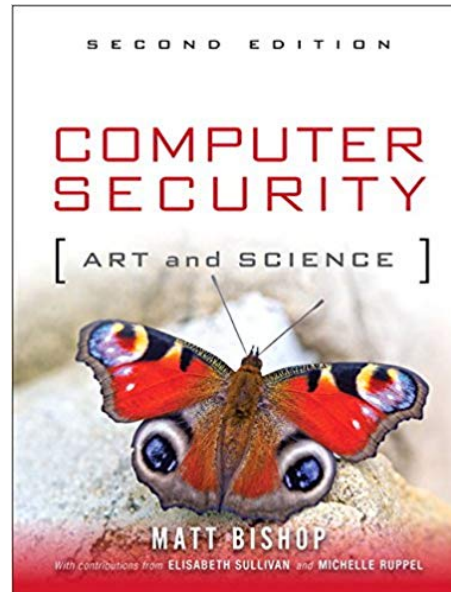Primary literature - not all chapters are curriculumr:

- *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
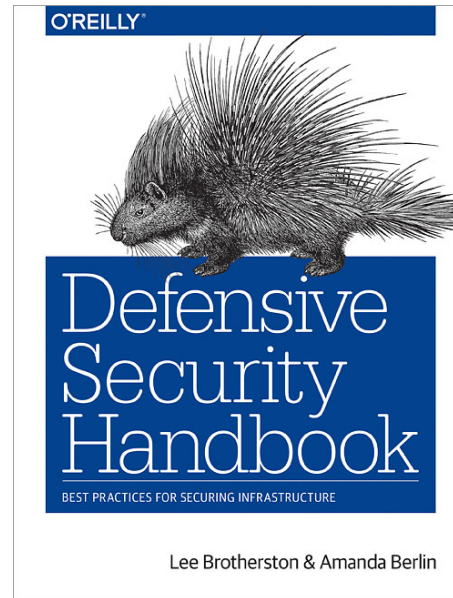
Free graphics by Lumen Design Studio

# Book: Computer Security: Art and Science



*Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332
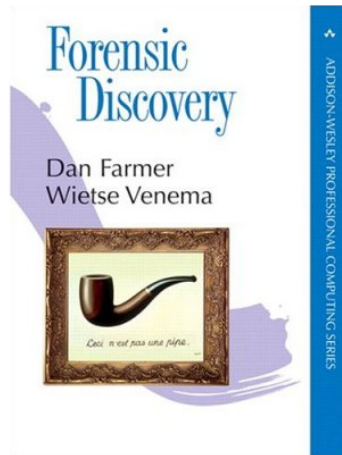
https://www.pearson.com/us/higher-education/program/Bishop-Computer-Security-2nd-Edition/PGM25107.html

# Book: Defensive Security Handbook (DSH)



*Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin ISBN: 978-1-491-96038-7
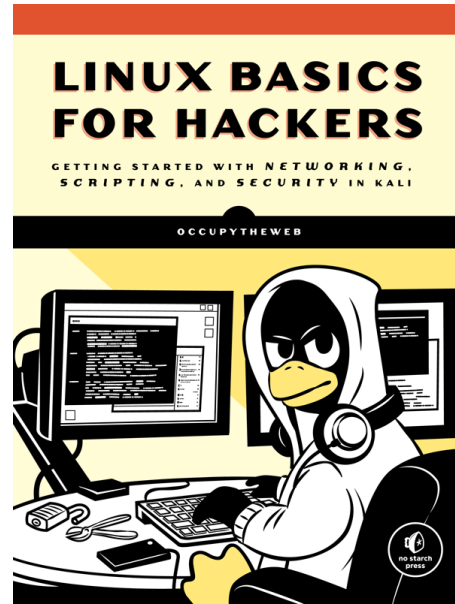
# Book: Forensics Discovery (FD)



*Forensics Discovery*, Dan Farmer, Wietse Venema 2004, Addison-Wesley.

Can be found at http://www.porcupine.org/forensics/forensic-discovery/ but recommend buying it - to support and also better formatted for reading
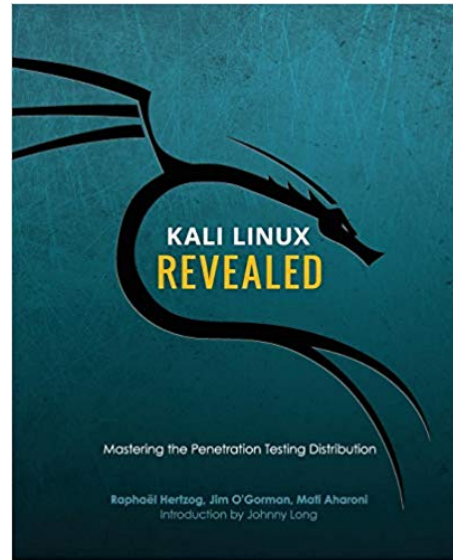
# Book: Linux Basics for Hackers (LBfH)



*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

# Book: Kali Linux Revealed (KLR)

*Kali Linux Revealed Mastering the Penetration Testing Distribution*

`https://www.kali.org/download-kali-linux-revealed-book/`
Not curriculum but explains how to install Kali Linux
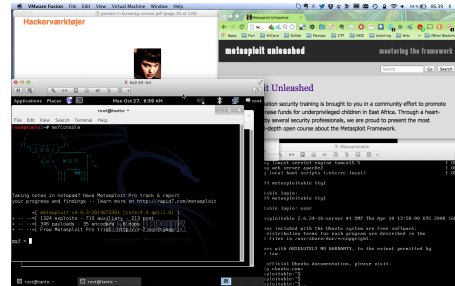
# Exercise



Now lets do the exercise

## Download Kali Linux Revealed (KLR) Book 10 min

which is number 1 in the exercise PDF.

# Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine amd64 64-bit `https://www.kali.org/`
- Linux server system: Debian 10 Buster amd64 64-bit `https://www.debian.org/`
- Setup instructions can be found at `https://github.com/kramse/kramse-labs`

It is enough if these VMs are pr team

# Aftale om test af netværk

**Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som ube-rettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.**

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: `http://www.stophacking.dk` lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

# Exercise
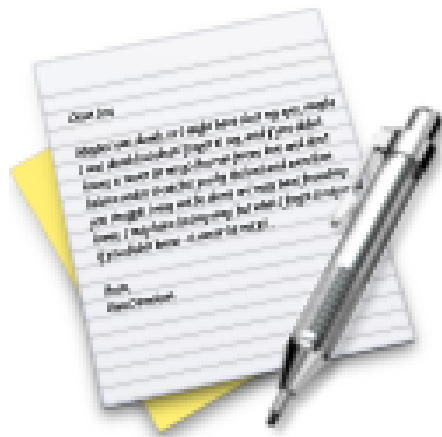
Now lets do the exercise

## Check your Kali VM, run Kali Linux 30 min

which is number **2** in the exercise PDF.

# Exercise



Now lets do the exercise

## Check your Debian VM 10 min

which is number **3** in the exercise PDF.

# Command prompt

We will use Unix/Linux systems, and you need to use the command line a bit:

```
[hlk@fischer hlk]$ id
uid=6000(hlk) gid=20(staff) groups=20(staff),
0(wheel), 80(admin), 160(cvs)
[hlk@fischer hlk]$

[root@fischer hlk]# id
uid=0(root) gid=0(wheel) groups=0(wheel), 1(daemon),
2(kmem), 3(sys), 4(tty), 5(operator), 20(staff),
31(guest), 80(admin)
[root@fischer hlk]#
```

$ is commonly used for showing a user login, while a # is for root logins

Change from user to root using the command sudo like sudo -s

# Command Syntax

A common syntax for commands are described like this:

```
echo [-n] [string ...]
```

- The command is the first thing on the command line, you cannot write `henrik echo`
- Options are prefixed with dash `-n`, optional ones are in brackets `[]`
- Multiple options can be combined into one group like, `tar -cvf` eller `tar cvf`
- Some options require arguments, like `tar -cf filename` where `-f` needs a filename

# Manual System

| kommando | [options] | [argumenter] |
|----------|-----------|--------------|
| $ cal | -j | 2005 |

It is a book about a Spanish guy called Manual. You should read it. – Dilbert

The Unix/Linux manual system is where you find the options, commands and file formats

Manuals must be installed, if not install them immediately

Very similar across Unix variants, OpenBSD is known for having an excellent manual pages

`man -k` allows keyword search similar can be done using `apropos`

Try `man crontab` and `man 5 crontab`

# Example Manual Page

```
NAME
     cal - displays a calendar
SYNOPSIS
     cal [-jy] [[month]  year]
DESCRIPTION
   cal displays a simple calendar.  If arguments are not specified, the cur-
   rent month is displayed.  The options are as follows:
   -j       Display julian dates (days one-based, numbered from January 1).
   -y       Display a calendar for the current year.

The Gregorian Reformation is assumed to have occurred in 1752 on the 3rd
of September.  By this time, most countries had recognized the reforma-
tion (although a few did not recognize it until the early 1900's.)  Ten
days following that date were eliminated by the reformation, so the cal-
endar for that month is a bit unusual.
```

# Unix Command Line Shells

- sh - Bourne Shell
- bash - Bourne Again Shell, often the default in Linux
- ksh - Korn shell, originally by David Korn, popular version `pdksh` public domain ksh
- csh - C shell, syntax close to the C programming language
- multiple others exist: zsh, tcsh

Comparable to command.com, cmd.exe and powershell in Windows

Also commonly used for small programs, scripts

When writing scripts use the characters number sign and exclamation mark (#!) in the beginning

See more in `https://en.wikipedia.org/wiki/Shell_(computing)`
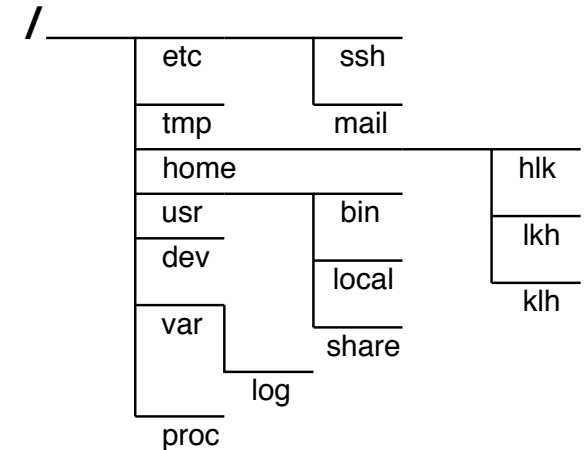`https://en.wikipedia.org/wiki/Shebang_(Unix)`
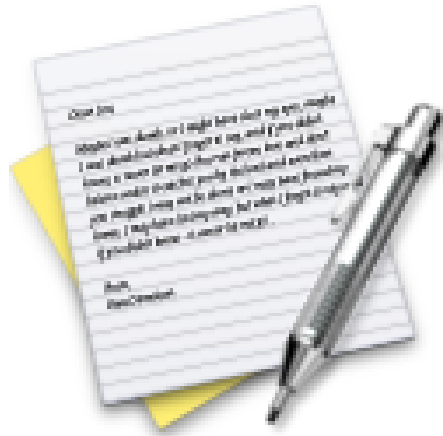
# Linux file system and konfiguration

.

- Unix/Linux uses a virtual filesystem
  `https://en.wikipedia.org/wiki/Unix_filesystem`
- No drive letters, just disks mounted in a common tree
- Everything starts with the file system root / - forward
- An important directory is /etc/ which includes a lot of configuration for the system and applications

```
/
├── etc ─── ssh
│          └── mail
├── tmp
├── home ──────────── hlk
├── usr ──── bin ──── lkh
├── dev      local ── klh
├── var      share
│   └── log
└── proc
```

# Exercise

Now lets do the exercise

## Investigate /etc 10 min

which is number **4** in the exercise PDF.

# For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books!