





Welcome to

0. Introduction

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse  

Slides are available as PDF, [kramse@Github](https://github.com/kramse/kramse@Github)
0-Introduction.tex in the repo [security-courses](https://github.com/kramse/security-courses)

Contact information



- Henrik Lund Kramshøj, internet samurai mostly networks and infosec
- Independent security consultant
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: [hlc@zencurity.dk](mailto:hk@zencurity.dk) Mobile: +45 2026 6000

You are welcome to drop me an email



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

Teaching dates: tuesdays and thursdays 23/04, 25/04, 30/04, 02/05, 07/05, 09/05, 14/05, 16/05, 21/05, 23/05, 28/05, 04/06, 06/06, 11/06, 13/06

Exam: tuesday 25/06 exam

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

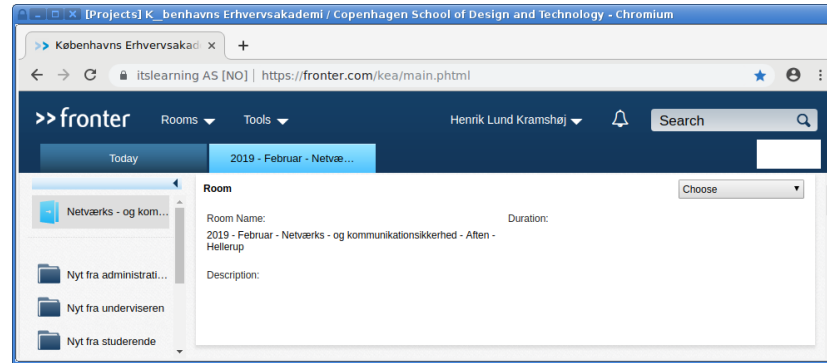
Note: the presentation slides are not a substitute for reading the books, papers and doing exercises, many details are not shown

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.

Frontier Platform



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

You will also be asked to turn in deliverables through frontier

<https://fronter.com/kea/main.phtml>

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

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

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

Expectations alignment



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

Primary literature



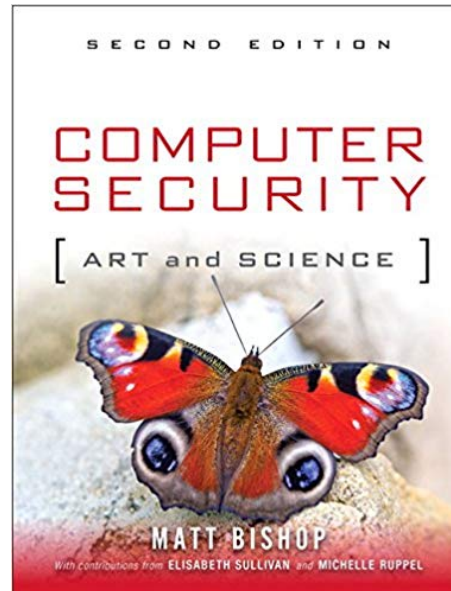
Primary literature:

- *Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332

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

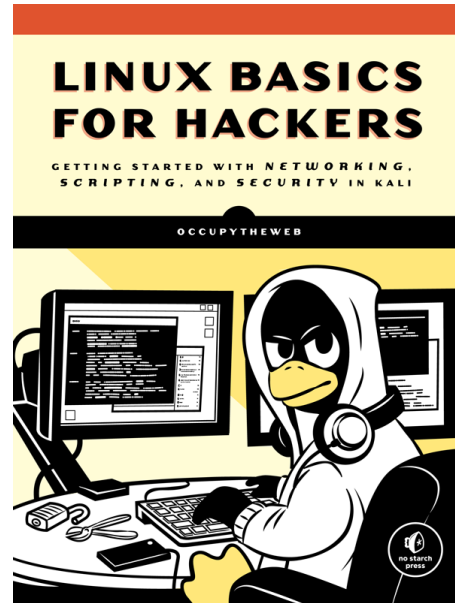
Book: Computer Security: Art and Science



Computer Security: Art and Science, Matt Bishop ISBN: 9780321712332

<https://nostarch.com/packetanalysis3>

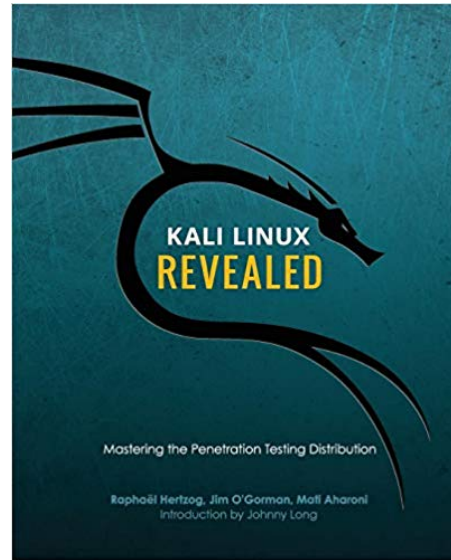
Book: Linux Basics for Hackers (LBhf)



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>

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

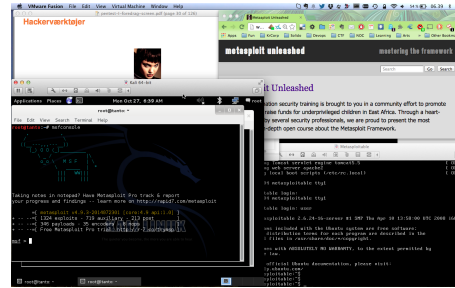


Now lets do the exercise

Download Kali Linux Revealed (KLR) Book 10 min

which is number **1** in the exercise PDF.

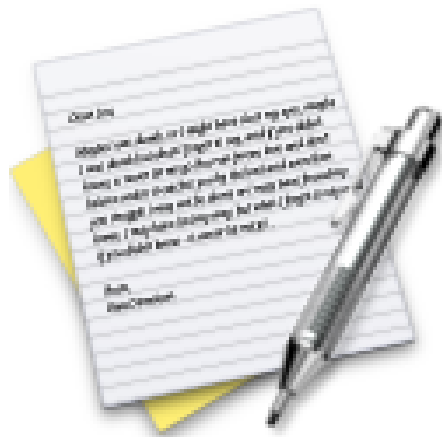
Hackertlab Setup



- Hardware: modern laptop CPU with virtualisation
Don't 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 9 Stretch 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

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

Bonus: Check your Debian VM 10 min

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

Manualsystemet



kommando [options] [argumenter]

\$ cal -j 2005

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

Manualsystemet i UNIX er utroligt stærkt!

Det SKAL altid installeres sammen med værktøjerne!

Det er næsten identisk på diverse UNIX varianter!

man -k søger efter keyword, se også apropos

Prøv man crontab og man 5 crontab

En manualside



NAME

`cal` - displays a calendar

SYNOPSIS

`cal [-jy] [[month] year]`

DESCRIPTION

`cal` displays a simple calendar. If arguments are not specified, the current 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 reformation (although a few did not recognize it until the early 1900's.) Ten days following that date were eliminated by the reformation, so the calendar for that month is a bit unusual.

Kommandolinien på UNIX



Shells kommandofortolkere:

- sh - Bourne Shell
- bash - Bourne Again Shell, ofte default på Linux
- ksh - Korn shell, lavet af David Korn
- csh - C shell, syntaks der minder om C sproget
- flere andre, zsh, tcsh

Svarer til `command.com` og `cmd.exe` på Windows

Kan bruges som komplette programmeringssprog

Kommandoprompten



```
[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]#
```

typisk viser et dollartegn at man er logget ind som almindelig bruger
mens en havelåge at man er root - superbruger

Kommandoliniens opbygning



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

Kommandoerne der skrives på kommandolinien skrives sådan:

- Starter altid med kommandoen, man kan ikke skrive `henrik echo`
- Options skrives typisk med bindestreg foran, eksempelvis `-n`
- Flere options kan sættes sammen, `tar -cvf` eller `tar cvf`
- I manualsystemet kan man se valgfrie options i firkantede klammer `[]`
- Argumenterne til kommandoen skrives typisk til sidst (eller der bruges redirection)

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Most days have about 100 pages or less, but one day has 4 chapters to read!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books!