Welcome to

0. Introduction

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

0-Introduction-software-security.tex in the repo 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: 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

Hardware

Since we are going to be doing exercises, each team will need two virtual machines.

The following are two recommended models:

- One based on Debian 9, running software servers and web applications
- One based on Kali Linux, running attacks against software

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

Course Materials

This material is in multiple parts:

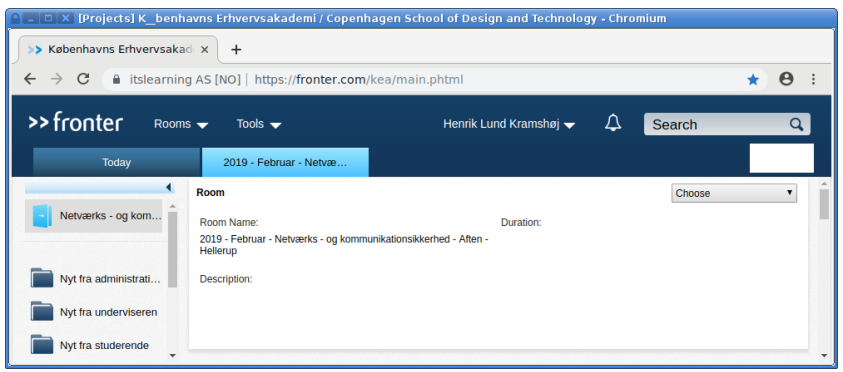
- Slide shows - presentation - this file
- Exercises - PDF which is updated along the way

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-software-security kramse@Github

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://fronter.com/kea/main.phtml`

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: Software Security
VF 3 Systemsikkerhed (10 ECTS)

Teaching dates: mostly tuesdays and thursdays 17:00 - 20:30
27/8 2019, 29/8 2019, 3/9 2019, 10/9 2019, 11/9 2019, 12/9 2019, 17/9 2019, 19/9 2019, 24/9 2019, 1/10 2019, 3/10 2019, 8/10 2019, 9/10 2019, 10/10 2019

Exam: tuesday 22/10 exam

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 Modulet fokuserer på sikkerhedsperspektivet i software, blandt andet programkvalitet og fejlhåndterings samt datahåndterings betydning for en software arkitekturs sårbarheder. Elementet introducerer også til forskellige design-principper, herunder "security by design".

Viden Den studerende har viden om:
Hvilken betydning programkvalitet har for it-sikkerhed ift.:

- Trusler mod software
- Kriterier for programkvalitet
- Fejlhåndtering i programmer
- Forståelse for security design principles, herunder:
- Security by design
- Privacy by design

Færdigheder Den studerende kan:
Tage højde for sikkerhedsaspekter ved at:

- Programmere håndtering af forventede og uventede fejl
- Definere lovlige og ikke-lovlige input data, bl.a. til test
- Bruge et API og/eller standard biblioteker
- Opdage og forhindre sårbarheder i programkoder
- Sikkerhedsvurdere et givet software arkitektur

Kompetencer Den studerende kan:

- Håndtere risikovurdering af programkode for sårbarheder.
- Håndtere udvalgte 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:

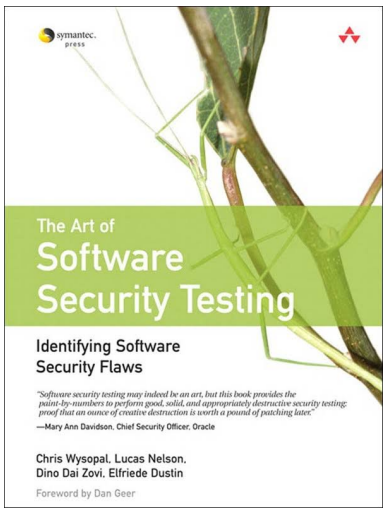
Free graphics by Lumen Design Studio

- *The Art of Software Security Testing Identifying Software Security Flaws* Chris Wysopal ISBN: 9780321304865, AoST or the Green Book
- *The Art of Software Security Assessment Identifying and Preventing Software Vulnerabilities* Mark Dowd, John McDonald, Justin Schuh ISBN: 9780321444424, AoSSA or the Red Book

Supporting literature:

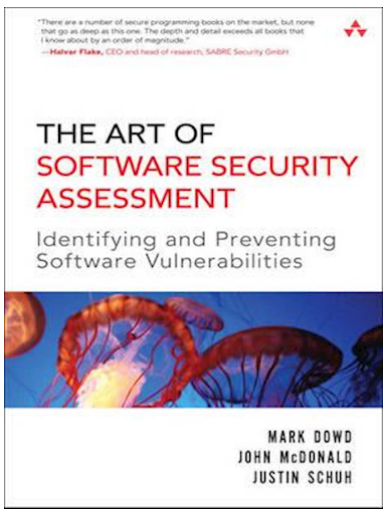
- *Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali*. OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7 - shortened LBfH
- *Kali Linux Revealed Mastering the Penetration Testing Distribution* Raphael Hertzog, Jim O'Gorman - shortened KLR

Book: The Art of Software Security Testing



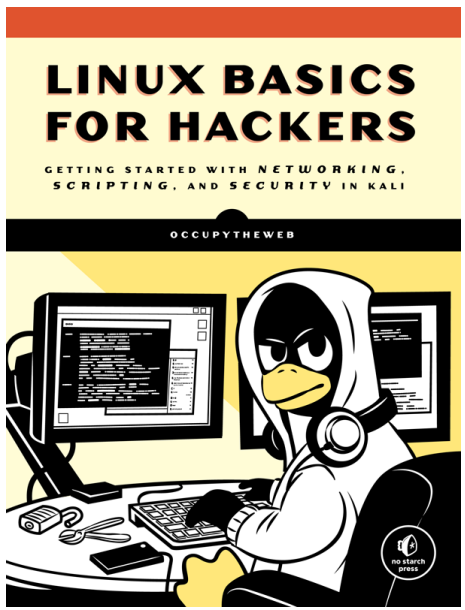
The Art of Software Security Testing Identifying Software Security Flaws
Chris Wysopal ISBN: 9780321304865, AoST or the Green Book

Book: The Art of Software Security Assessment



The Art of Software Security Assessment Identifying and Preventing Software Vulnerabilities
Mark Dowd, John McDonald, Justin Schuh ISBN: 9780321444424, AoSSA or the Red Book

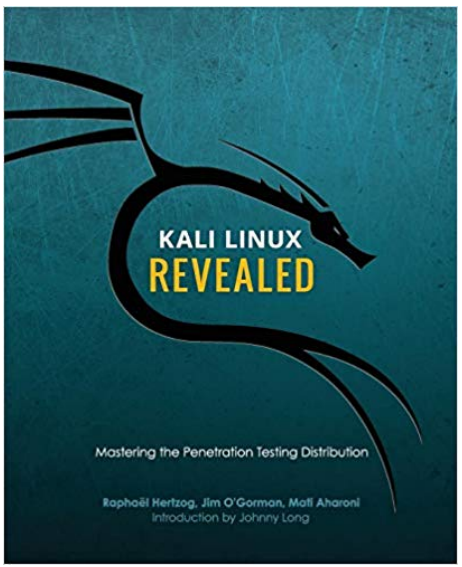
Book: Linux Basics for Hackers (LBhf)



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` Not curriculum but explains how to use Linux

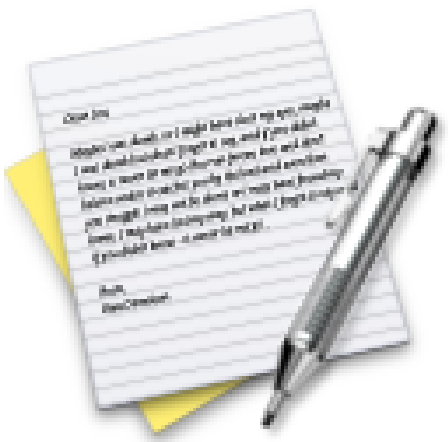
Book: Kali Linux Revealed (KLR)



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

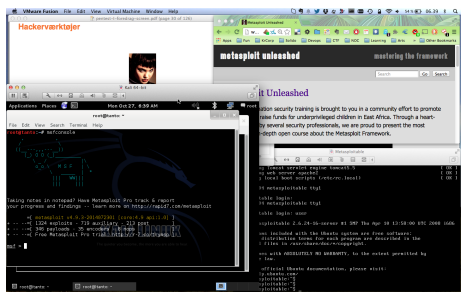


Now lets do the exercise

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 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

OWASP Juice Shop Project

We will also use the OWASP Juice Shop Tool Project as a running example. This is an application which is modern AND designed to have security flaws.

Read more about this project at: `https://www.owasp.org/index.php/OWASP_Juice_Shop_Project` `https://github.com/bkimminich/juice-shop`

It is recommended to buy the Pwning OWASP Juice Shop Official companion guide to the OWASP Juice Shop from `https://leanpub.com/juice-shop` - suggested price USD 5.99

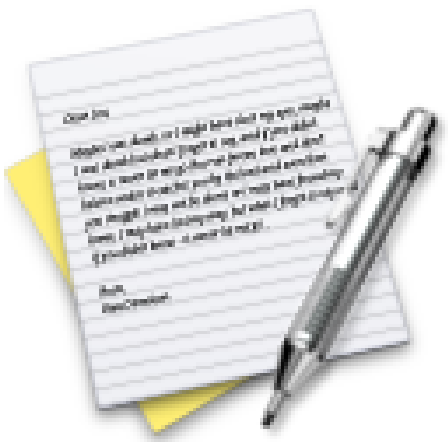
Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget 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

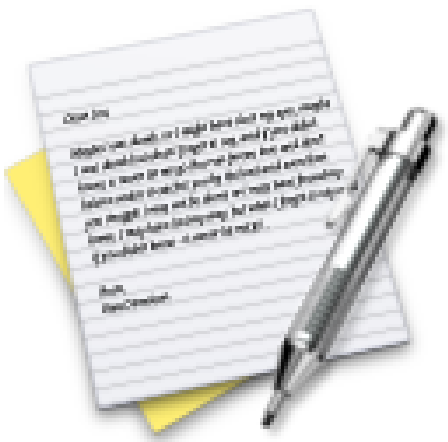


Now lets do the exercise

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.

Kommandoprompten

```
[hlk@fischer hlk]$ id
uid=6000(hlk) gid=20(staff) groups=20(staff),
0(wheel), 80(admin), 160(cvs)
[hlk@fischer hlk]$ sudo -s
[root@fischer hlk]#
[root@fischer hlk]# id
uid=0(root) gid=0(wheel) groups=0(wheel), 1(daemon),
20(staff), 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

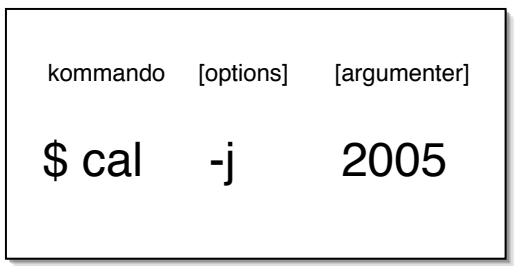
Kommandoliniens opbygning

```
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)

Manualsystemet



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 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.
```

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

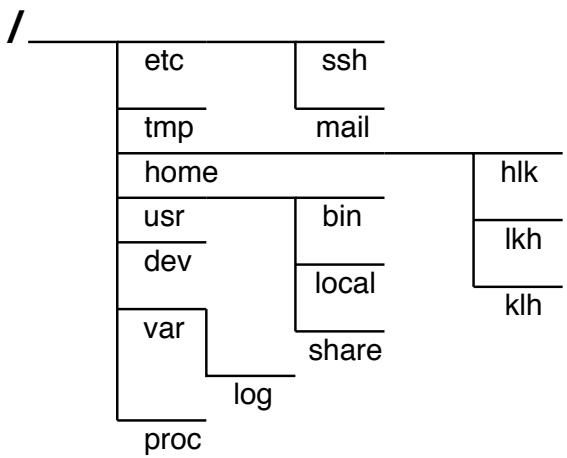
Svarer til command.com og cmd.exe på Windows

Kan bruges som komplette programmeringssprog

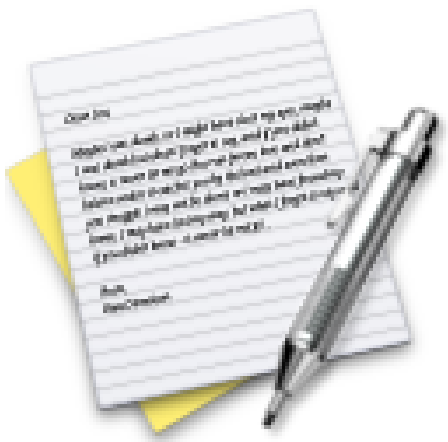
Linux konfiguration /etc

.

- Kommandolinien er et krav i studieordningen ☺
- Linux og Unix bruger et fælles fil-system
  `https://en.wikipedia.org/wiki/Unix_filesystem`
- Der er ingen drev-bogstaver som man kender fra MS-DOS og Microsoft Windows
- Alt starter ved roden / - *forward slash*
- Kataloget `/etc/` og underkataloger indeholder det meste konfiguration, derfor særligt interessant for sikkerheden



Exercise



Now lets do the exercise

Investigate /etc 10 min

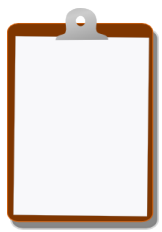
which is number **4** in the exercise PDF.

Course overview

We will now go through the Table of Contents in the books.

and the *Lektionsplan*
`https://zencurity.gitbook.io/kea-it-sikkerhed/softwaresikkerhed/lektionsplan`

For Next Time



Think about the subjects from this time, write down questions

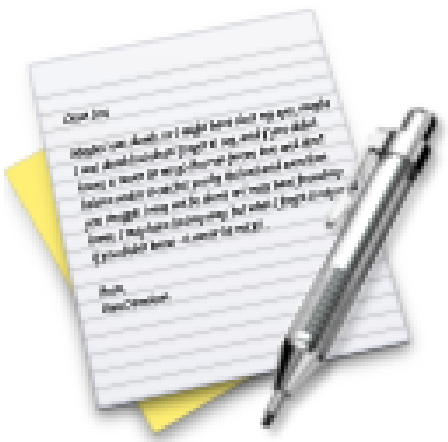
Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books!

Exercise



Now lets do the exercise

Run OWASP Juice Shop

which is number **5** in the exercise PDF.