




Welcome to

## 0. Introduction

# KEA Kompetence SIEM and Log Analysis

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

Slides are available as PDF, [kramse@Github](mailto:kramse@Github)

0-Introduction-siem-log-analysis.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: [hkj@zencurity.dk](mailto:hkj@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 systems:

- One based on Debian, running software servers and web applications
- Setup instructions and help <https://github.com/kramse/kramse-labs>

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

# Course Materials



This material is in multiple parts:

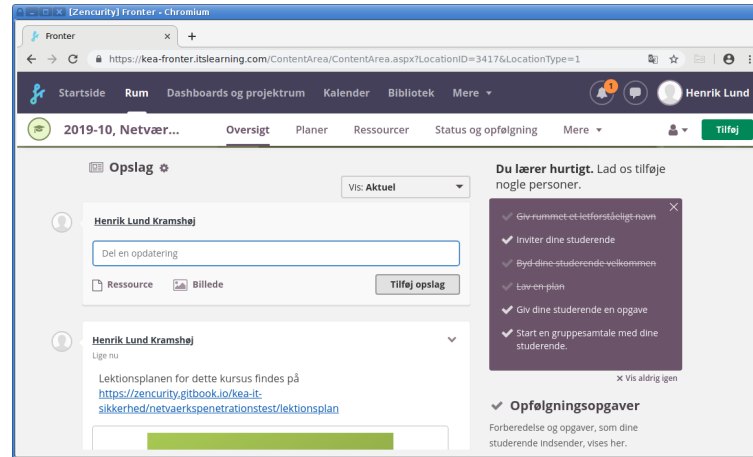
- Slide shows - presentation - this file
- Exercises - PDF which is updated along the way

Books listed in the lecture plan and here

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

# 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: SIEM and Log Analysis (5 ECTS)

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

26/11 2020, 1/12 2020, 3/12 2020, 8/12 2020, 10/12 2020, 15/12 2020, 17/12 2020

Exam: 7/1 2021



# 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:
- 1 Mandatory assignments
- Mandatory assignments are required in order to be entitled to the exam.

# Course Description



From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018  
VF4 SIEM og log analyse (5 ECTS)

## Indhold

Den studerende lærer om Security information and event management (SIEM), herunder hvordan man kan indsamle, administrere, og søge i sikkerhedshændelsesdata i et større it system (komplekse systemer, IOT deployments, corporate IT).

## Læringsmål

Viden – Den studerende har viden om og forståelse for:

- Typiske SIEM arkitekturer
- Standard logformater og logtyper for standard systemer og komponenter
- Typiske SIEM produkter
- Juridiske krav til logning og bevarelse af data ifb. forensic analyse

Færdigheder – Den studerende kan:



- Lave en baseline-analyse af en infrastruktur
- Bruge log-data til at identificere infrastrukturkomponenter
- Bruge et værktøj til at analysere system log-data og netværkstrafik til at finde sikkerhedshændelser
- Udvikle "dashboards" og alarmer der viser tegn på hændelser

Kompetencer – Den studerende kan:

- Designe og implementere en SIEM løsning på tværs af diverse produkter
- Træffe beslutninger om hvilke data der skal indsamles i en givne situation
- Identificerer fejl i logopsamlingen
- Deltage i drøftelser på et praktisk og strategisk niveau i forhold til implementering af logmanagement/SIEM

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 10 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

I look forward to hearing your wishes, and hopefully we can accomodate some

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

# Goals and plans



“A goal without a plan is just a wish.”

Antoine de Saint-Exupéry

I want this course to

- Include everything required by studieordningen
- Be practical – you can do something useful
- Kickstart your journey into SIEM and Logging
  - Getting the best books with pointers about the closely related subject incident response
- Present a lot of useful sources, data types, tools
- Prepare you for production use of the knowledge
  - Example you can take Linux, Ansible and Elasticsearch almost directly into production

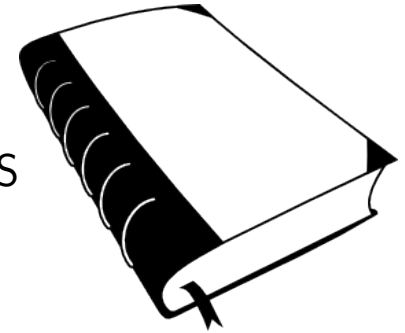
We only have 5 ECTS, but a lot of flexibility.

# Primary literature



Primary literature:

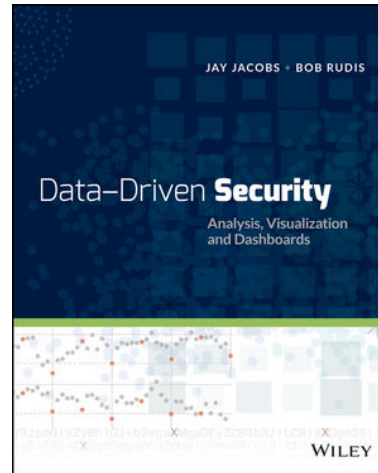
- *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis  
ISBN: 978-1-118-79372-5 February 2014 <https://datadrivensecurity.info/> - short DDS
- *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*  
by Jeff Bollinger, Brandon Enright, and Matthew Valites - short CIP
- *Intelligence-Driven Incident Response* ISBN: 9781491934944  
Scott Roberts - short IDI
- *Security Operations Center: Building, Operating, and Maintaining your SOC*  
ISBN: 9780134052014 Joseph Muniz - short SOC



Free graphics by Lumen Design Studio

Problem: You probably dont have the books yet ...

# Book: Data-Driven Security: Analysis, Visualization and Dashboards



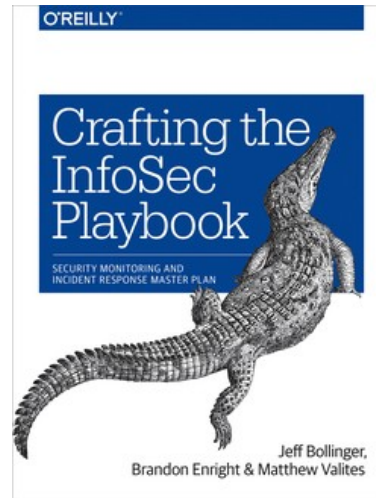
*Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis

ISBN: 978-1-118-79372-5 February 2014 <https://datadrivensecurity.info/> - short DDS

Our main book for this course. We will read a lot from this one.

Note: they also have quite a lot of blog posts available, updates since the book came out and until 2016

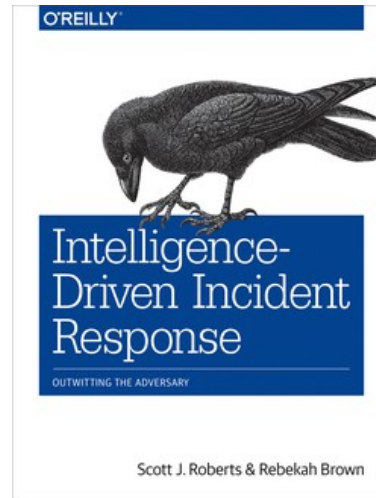
# Book: Crafting the InfoSec Playbook



*Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*  
by Jeff Bollinger, Brandon Enright, and Matthew Valites - short CIP



# Book: Intelligence-Driven Incident Response



*Intelligence-Driven Incident Response* ISBN: 9781491934944

Scott Roberts - short IDI

# Book: Security Operations Center



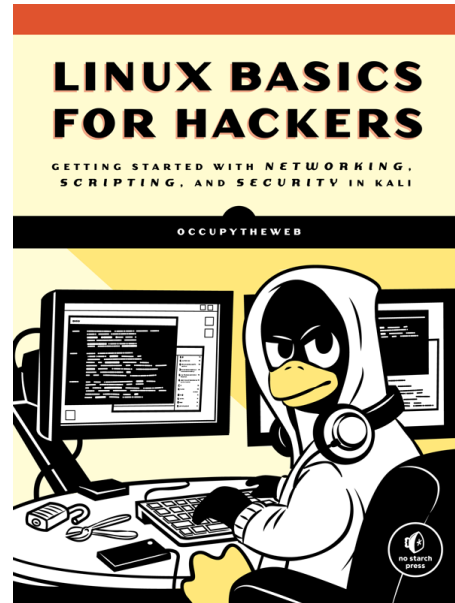
*Security Operations Center: Building, Operating, and Maintaining your SOC*  
ISBN: 9780134052014 Joseph Muniz - short SOC

# Supporting literature books



- *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
- *The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas  
<https://debian-handbook.info/> - shortened DEB
- *Kali Linux Revealed Mastering the Penetration Testing Distribution*  
Raphaël Hertzog, Jim O'Gorman - shortened KLR

# 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

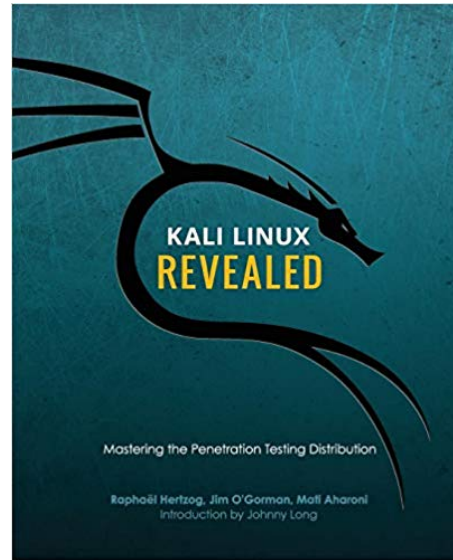
## Book: The Debian Administrator's Handbook (DEB)



*The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas  
<https://debian-handbook.info/> - shortened DEB

Not curriculum but explains how to use Debian Linux

## Book: Kali Linux Revealed (KLR)

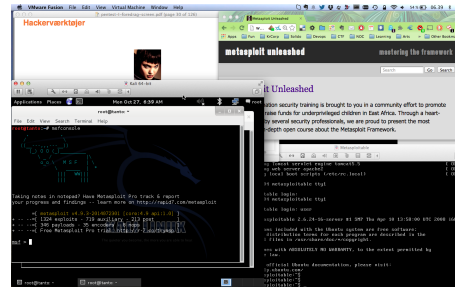


*Kali Linux Revealed Mastering the Penetration Testing Distribution*

<https://www.kali.org/download-kali-linux-revealed-book/>

Not curriculum but explains how to install Kali Linux

# 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
- Linux server system: Debian 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

# Command prompts in Unix



## Shells :

- sh - Bourne Shell
- bash - Bourne Again Shell, often the default in Linux
- ksh - Korn shell, original by David Korn, but often the public domain version used
- csh - C shell, syntax similar to C language
- Multiple others available, zsh is very popular

Windows have `command.com`, `cmd.exe` but PowerShell is more similar to the Unix shells

Used for scripting, automation and programs



# Command prompts



```
[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]#
```

Note the difference between running as root and normal user. Usually books and instructions will use a prompt of hash mark # when the root user is assumed and dollar sign \$ when a normal user prompt.

# Command syntax



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

Commands are written like this:

- Always begin with the command to execute, like `echo` above
- Options typically short form with single dash `-n`
- or long options `--version`
- Some commands allow grouping options, `tar -c -v -f` becomes `tar -cvf`  
NOTE: some options require parameters, so `tar -c -f filename.tar` not equal to `tar -fc filename.tar`
- Optional options are in brackets `[ ]`
- Output can be saved using redirection, into new file/overwrite `echo hello > file.txt` or append `echo hello >> file.txt`
- Read from files `wc -l file.txt` or pipe output into input `cat file.txt | wc -l`  
`wc` is word count, and option `l` is count lines

# Unix Manual system



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

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

Manual system in Unix is always there!

Key word search `man -k` see also `apropos`

Different sections, can be chosen

See `man crontab` the command vs the file format in section 5 `man 5 crontab`

# A manual page



## 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.

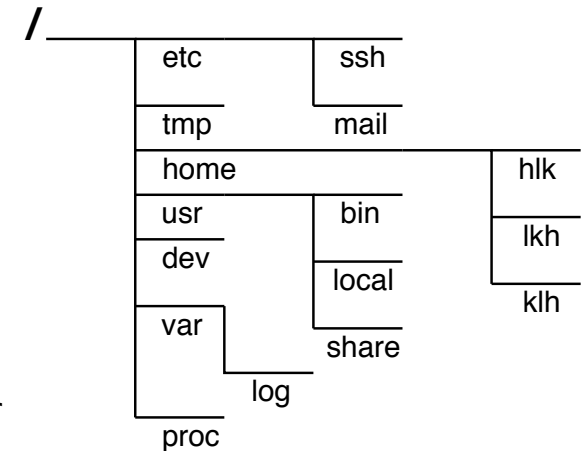
The Gregorian Reformation is assumed to have occurred in 1752 on the 3rd of September. By this time, most countries had recognized the reformation (although a few did not recognize it until the early 1900's.) Ten days following that date were eliminated by the reformation, so the calendar for that month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

# Linux configuration in /etc



.

- Command line is a requirement in the *studieordningen* 😊
- Linux and Unix uses a single virtual file system  
[https://en.wikipedia.org/wiki/Unix\\_filesystem](https://en.wikipedia.org/wiki/Unix_filesystem)
- No drive letters like the ones in MS-DOS and Microsoft Windows
- Everything starts at the root of the file system tree / - NOTE: *forward slash*
- One special directory is /etc/ and sub directories which usually contain a lot of configuration files



# Installing software in Debian – apt



## DESCRIPTION

apt provides a high-level commandline interface for the package management system. It is intended as an end user interface and enables some options better suited for interactive usage by default compared to more specialized APT tools like apt-get(8) and apt-cache(8).

### update (apt-get(8))

update is used to download package information from all configured sources. Other commands operate on this data to e.g. perform package upgrades or search in and display details about all packages available for installation.

### upgrade (apt-get(8))

upgrade is used to install available upgrades of all packages currently installed on the system from the sources configured via sources.list(5). New packages will be installed if required to satisfy dependencies, but existing packages will never be removed. If an upgrade for a package requires the removal of an installed package the upgrade for this package isn't performed.

### full-upgrade (apt-get(8))

full-upgrade performs the function of upgrade but will remove currently installed packages if this is needed to upgrade the system as a whole.

- Install a program using apt, for example `apt install nmap`

# Exercise



Now lets do the exercise

## Download Debian Administrator's Handbook (DEB) Book 10 min

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

# Exercise



Now lets do the exercise

## Check your Debian VM 10 min

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



# Exercise



Now lets do the exercise

**Investigate /etc 10 min**

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

# Course overview



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

and the *Lektionsplan*

<https://zencurity.gitbook.io/kea-it-sikkerhed/siem-and-log-analysis/lektionsplan>

# Mixed exercises



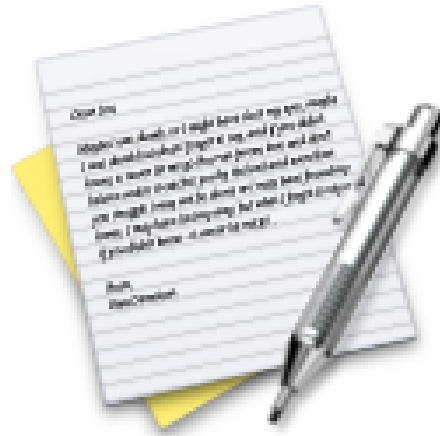
Then we will do a mixed bag of exercises to introduce technologies, find your current knowledge level with regards to:

- Linux
- Linux command line
- Python
- Data types
- Elasticsearch – how to run a *service*
- Running Java on Linux – environment variables?!
- Ansible provisioning – installing and configuring software for production

**Note: today we will consider all these optional, we wont be able to do them all**

Later we will return to them!

# Exercise

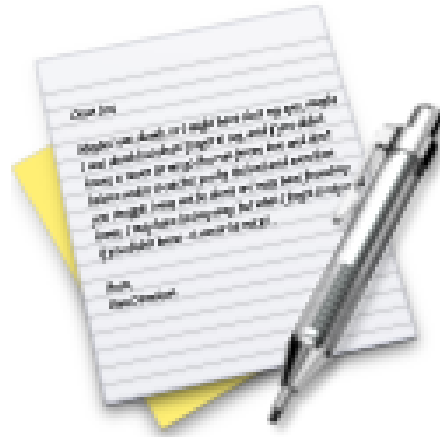


Now lets do the exercise

## Enable UFW firewall

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

# Exercise

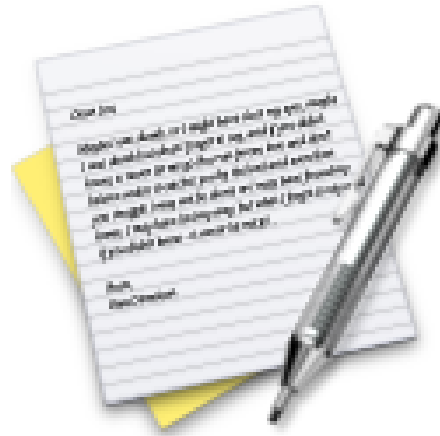


Now lets do the exercise

## Data types – IP addresses 15min

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

# Exercise



Now lets do the exercise

## Postman API Client 20 min

which is number **6** in the exercise PDF.

# Exercise



Now lets do the exercise

## Use Ansible to install Elastic Stack

which is number **7** in the exercise PDF.

# Exercise



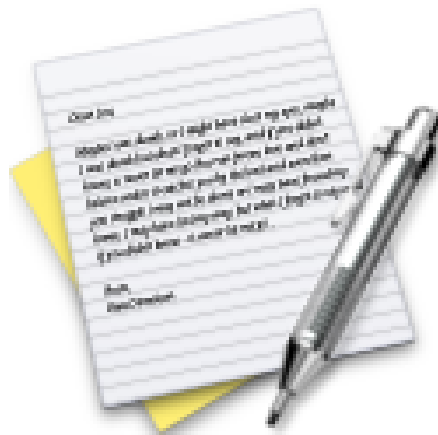
Now lets do the exercise

## Getting started with the Elastic Stack - 60 min

which is number **8** in the exercise PDF.



# Exercise



Now lets do the exercise

## Making requests to Elasticsearch - 15-75min

which is number **9** in the exercise PDF.

# Exercise

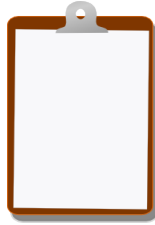


Now lets do the exercise

## Use a XML library in Python up to 60min

which is number **10** 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!