





Welcome to

0. Introduction

Communication and Network Security 2021

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse  

Slides are available as PDF, kramse@Github
0-Introduction.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 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



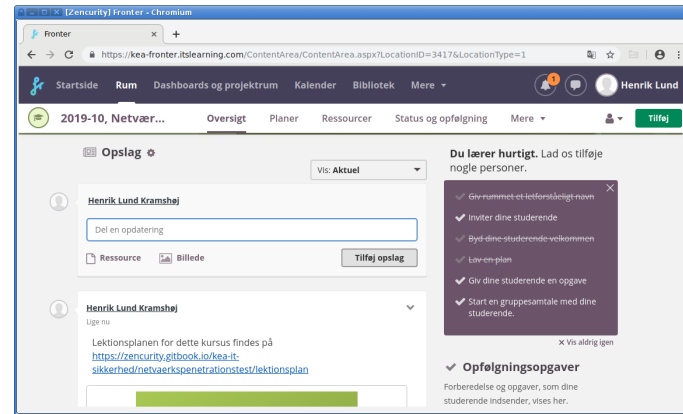
This material is in multiple parts:

- 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

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



Course: Communication and Network Security

Ob 1 Netværks- og kommunikationssikkerhed (10 ECTS)

Exam: Date June 11. 2020

Teaching dates: 14/4 2020, 16/4 2020, 21/4 2020, 23/4 2020, 28/4 2020, 30/4 2020, 5/5 2020, 7/5 2020, 12/5 2020, 14/5 2020, 19/5 2020, 20/5 2020, 26/5 2020, 28/5 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:

Modulet går ud på at forstå og håndtere netværkssikkerhedstrusler samt implementere og konfigurere udstyr til samme.

Modulet omhandler forskellig sikkerhedsudstyr (IDS) til monitorering. Derudover vurdering af sikkerheden i et netværk, udarbejdelse af plan til at lukke eventuelle sårbarheder i netværket samt gennemgang af forskellige VPN teknologier.

My translation:

The module is centered around network threats and implementing and configuring equipment in this area.

Module includes different security equipment like IDS for monitoring. The evaluation of security in a network, developing plans for closing security vulnerabilities in the network and a review of various VPN technologies.

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



My overall goal

- Introduce networking and related security issues
- Introduce resources, programs, people, authors, documents, sites that further your exploration into network security

Please brainstorm for 5 minutes on what topics you would like to have in this course, and write them down on a piece of paper or note program.

Decide on 5 topics and prioritize these 5 topics

and we will have a common presentation and write them down.

Prerequisites



This course includes exercises and getting the most of the course requires the participants to carry out these practical exercises

We will use Kali Linux for the exercises but previous Linux and Unix knowledge is not needed

It is recommended to use virtual machines for the exercises

Network security and most internet related security work has the following requirements:

- Network experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill**
 - too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

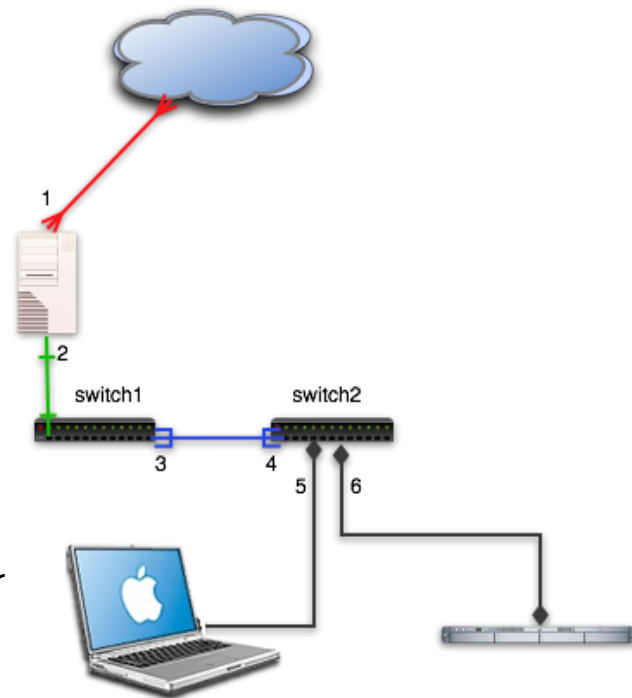
Course Network



I have a course network with me when needed, which has the following systems:

- OpenBSD router
- Switches Juniper EX2200-C and small TP-Link
- UniFi AP wireless access-point

This will be at my home, and due to remote teaching - we will investigate your networks and scan across the internet to *my servers*!



Primary literature

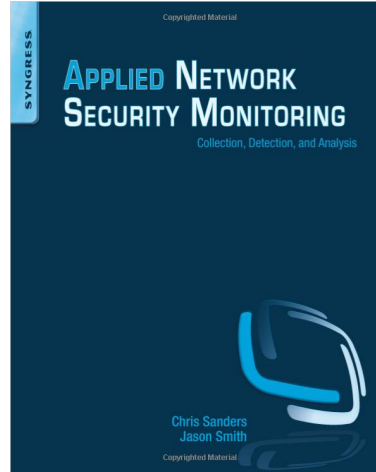


Primary literature are these three books:

- *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

Price check around January 2019 - all three can be bought in hardcopy for 1.000-1.100DKK

Book: Applied Network Security Monitoring (ANSM)

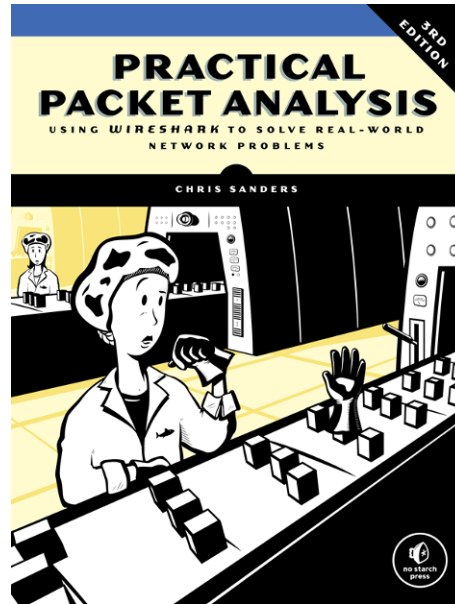


Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition

Chris Sanders, Jason Smith eBook ISBN: 9780124172166 Paperback ISBN: 9780124172081 496 pp. Imprint: Syngress, December 2013

<https://www.elsevier.com/books/applied-network-security-monitoring/unknown/978-0-12-417208-1>

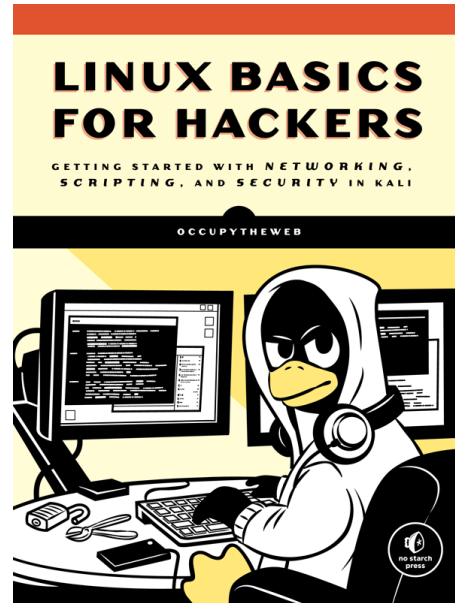
Book: Practical Packet Analysis (PPA)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1

<https://nostarch.com/packetanalysis3>

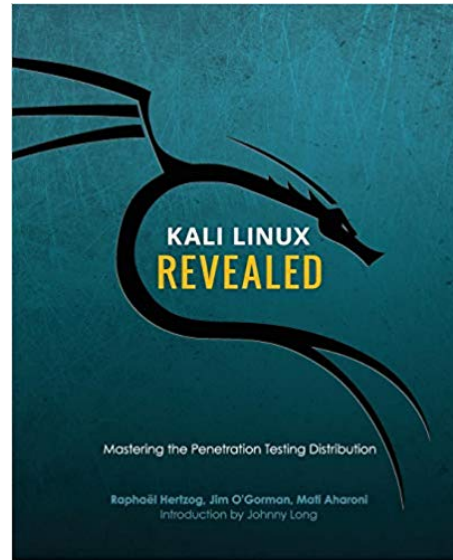
Book: Linux Basics for Hackers (LBhf)



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)

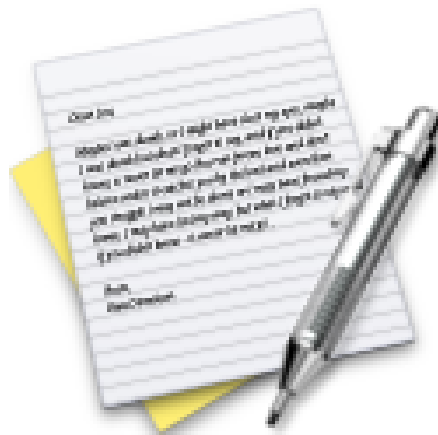


Kali Linux Revealed Mastering the Penetration Testing Distribution

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

Not curriculum but explains how to install Kali Linux

Exercise

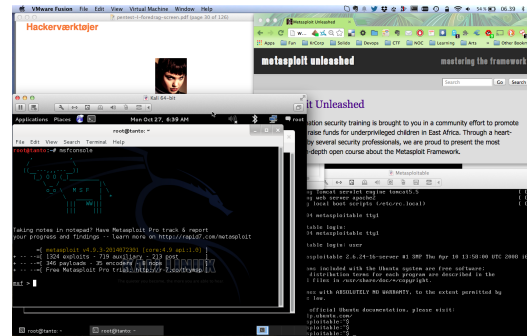


Now lets do the exercise

Download Kali Linux Revealed (KLR) Book 10 min

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

Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation
Dont forget to enable hardware virtualisation in the BIOS
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine <https://www.kali.org/>
- Soft targets: Metasploitable, Windows 2000, Windows XP, ...

Having a Debian VM will also be recommended, one pr team

Wifi Hardware



Since we are going to be doing exercises, sniffing data it will be an advantage to have a wireless USB network card.

- The following are two recommended models:
- TP-link TL-WN722N hardware version 2.0 cheap but only support 2.4GHz
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing
- Both work great in Kali Linux for our purposes.

I have some available for teams if you dont buy them.



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

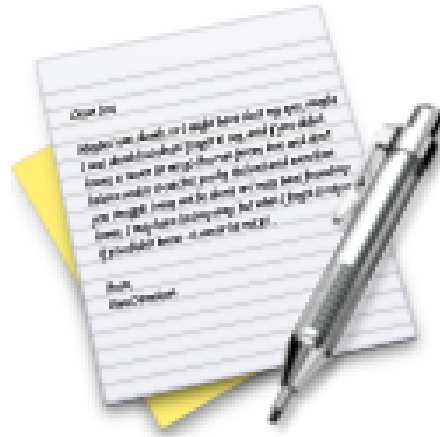


Now lets do the exercise

Check your Kali VM, run Kali Linux 30 min

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

Exercise



Now lets do the exercise

Bonus: Check your Debian VM 10 min

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

Access Unix



Access to Unix and Linux today typically uses a Windowing system, window manager and has evolved into large environments with base applications:

- KDE <http://www.kde.org>
- GNOME <http://www.gnome.org>
- Xfce <https://xfce.org/>

or the command line, terminals

Running commands on the command line



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

Commands writing on the command line are written like this:

- Commands are first, the order matters you cannot reverse them like: `henrik echo`
- Options most often written with a dash, like `-n`
- Multiple options can often be collapsed, `tar -cvf` eller `tar cvf`
Just notice some uses an argument too. The example `-f` needs a filename!
- In the manual system optional arguments are in brackets `[]`
- The arguments for the program then comes after the options and typically also are ordered

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/Shell_(computing))

[https://en.wikipedia.org/wiki/Shebang_\(Unix\)](https://en.wikipedia.org/wiki/Shebang_(Unix))

Command prompts



```
[h1k@fischer h1k]$ id
uid=6000(h1k) gid=20(staff) groups=20(staff),
0(wheel), 80(admin), 160(cvs)
[h1k@fischer h1k]$
```

```
[root@fischer h1k]# 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 h1k]#
```

When showing a dollar sign you are logged in as a regular user
while a hash mark means you are the root - super user, no restrictions

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 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.

The year 1752



```
user@Projects:communication-and-network-security$ cal 1752
```

...

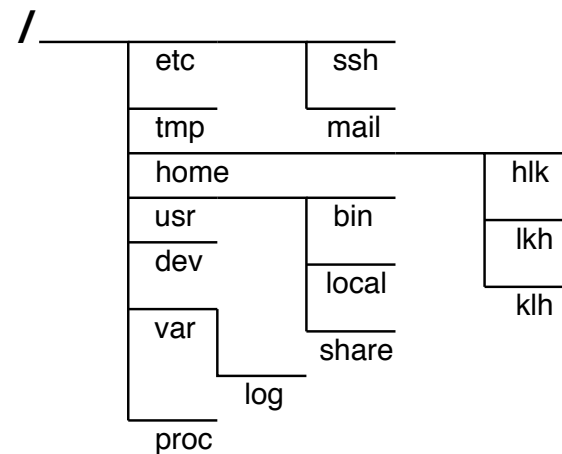
April							May							June						
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4						1	2		1	2	3	4	5	6
5	6	7	8	9	10	11	3	4	5	6	7	8	9	7	8	9	10	11	12	13
12	13	14	15	16	17	18	10	11	12	13	14	15	16	14	15	16	17	18	19	20
19	20	21	22	23	24	25	17	18	19	20	21	22	23	21	22	23	24	25	26	27
26	27	28	29	30			24	25	26	27	28	29	30	28	29	30				
							31													
July							August							September						
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4							1			1	2	14	15	16
5	6	7	8	9	10	11	2	3	4	5	6	7	8	17	18	19	20	21	22	23
12	13	14	15	16	17	18	9	10	11	12	13	14	15	24	25	26	27	28	29	30
19	20	21	22	23	24	25	16	17	18	19	20	21	22							
26	27	28	29	30	31		23	24	25	26	27	28	29							
							30	31												

...

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



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!