Welcome to

Introduction

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

0-Introduction.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

Course: Communication and Network Security
Ob 1 Netværks- og kommunikationssikkerhed (10 ECTS)

15 days of teaching

Exam: Date April 9. 2019

Teaching dates: 05/02 2019, 07/02 2019, 12/02 2019, 14/02 2019, 19/02 2019, 21/02 2019, 26/02 2019, 28/02 2019, 05/03 2019, 07/03 2019, 12/03 2019, 14/03 2019, 19/03 2019, 21/03 2019, 26/03 2019

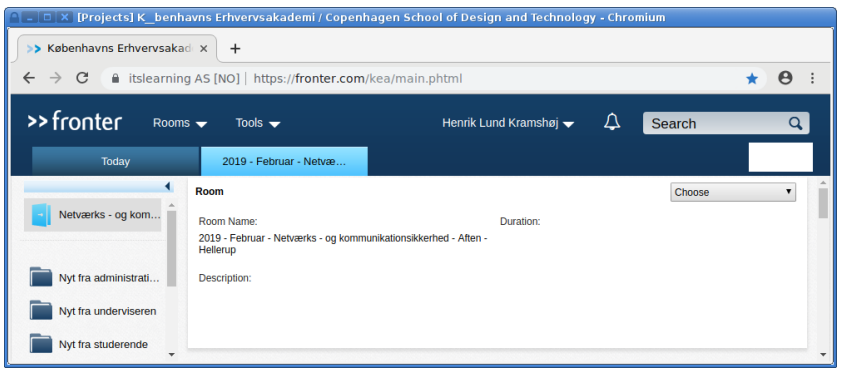
Changes: the dates 19/3 and 21/3 will be moved!
And since we are here, lets try to agree on best dates

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.

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

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

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

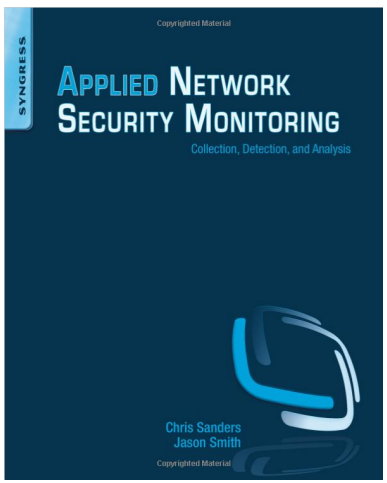
Primary literature

Primary literature 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 by 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)

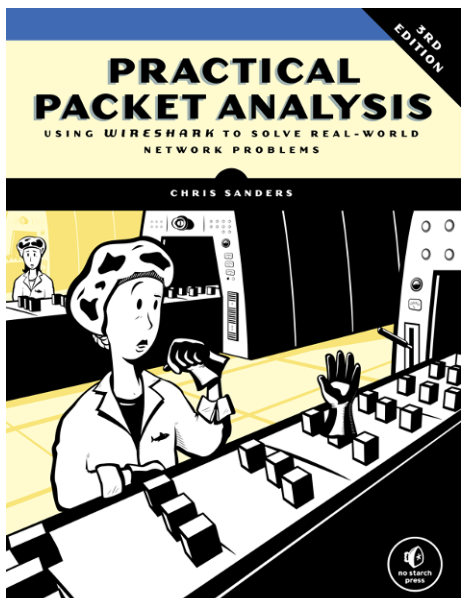


Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition

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`

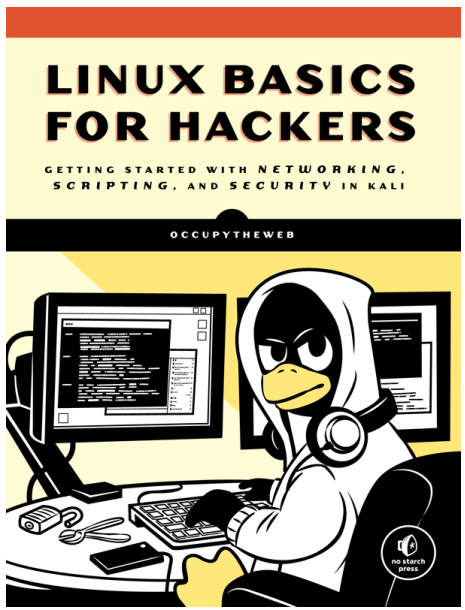
Book: Practical Packet Analysis (PPA)



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`

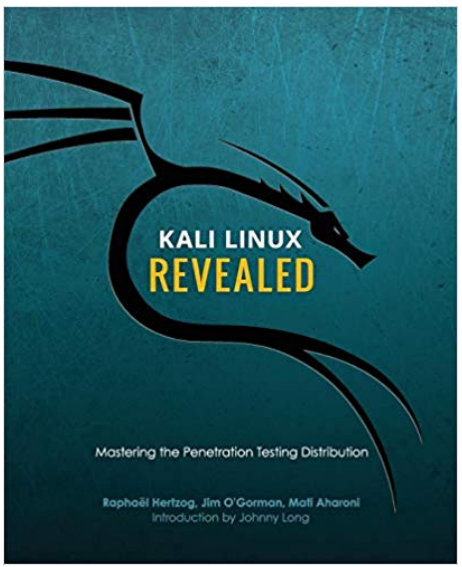
Book: Linux Basics for Hackers (LBhf)



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`

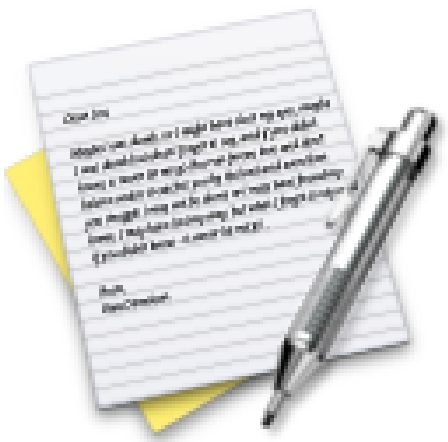
Book: Kali Linux Revealed (KLR)



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

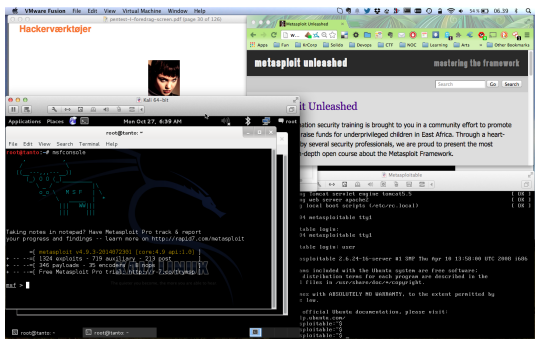


Now lets do the exercise

Download Kali Linux Revealed (KLR) Book

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 9 Stretch will also be recommended, one pr team

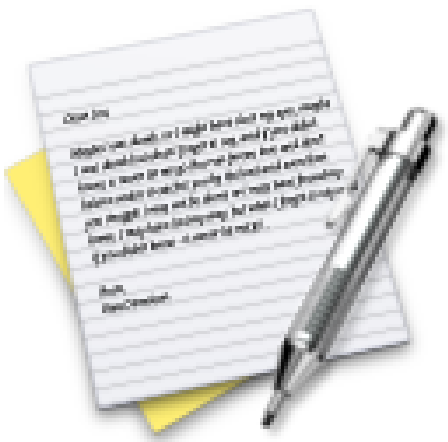
Wifi Hardware

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.

Exercise

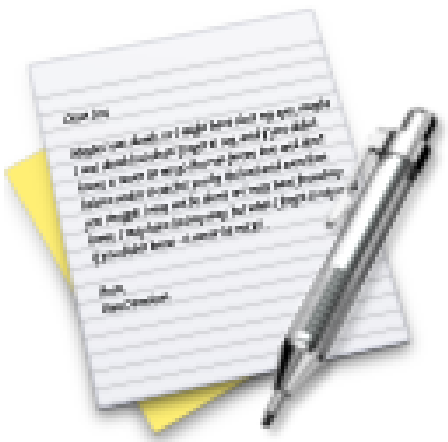


Now lets do the exercise

Check your Kali VM, run Kali Linux

which is number 2 in the exercise PDF.

Exercise

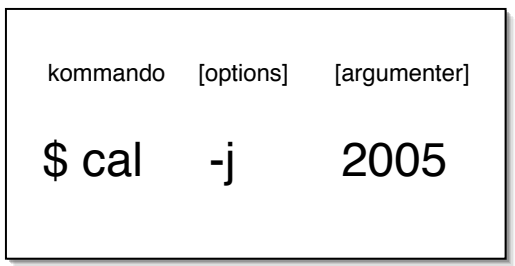


Now lets do the exercise

Bonus: Check your Debian VM

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

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

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)

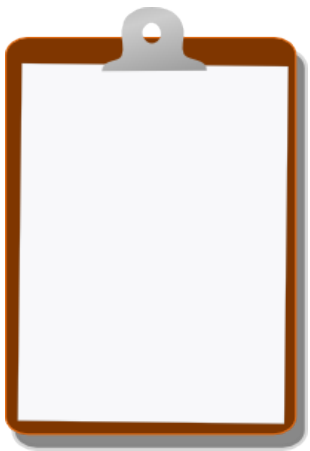
Adgang til UNIX

Adgang til UNIX kan ske via grafiske brugergrænseflader, eksempelvis

- KDE `http://www.kde.org`
- GNOME `http://www.gnome.org`

eller kommandolinien

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