Welcome to

0. Introduction

KEA Kompetence Penetration Testing

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

0-Introduction-kea-pentest.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

Course: Penetration testing
VF 3 Netværkspenetrationstest (5 ECTS)

Exam date: 24/11 2020

Teaching dates:
22/10 2020, 27/10 2020, 29/10 2020, 3/11 2020, 5/11 2020, 10/11 2020, 12/11 2020

Kursusmateriale

Dette materiale består af flere dele:

- Kursusmaterialet - præsentationen til undervisning - dette sæt
- Øvelseshæfte med øvelser

Hertil kommer diverse ressourcer fra internet, specielt RFC-dokumenter

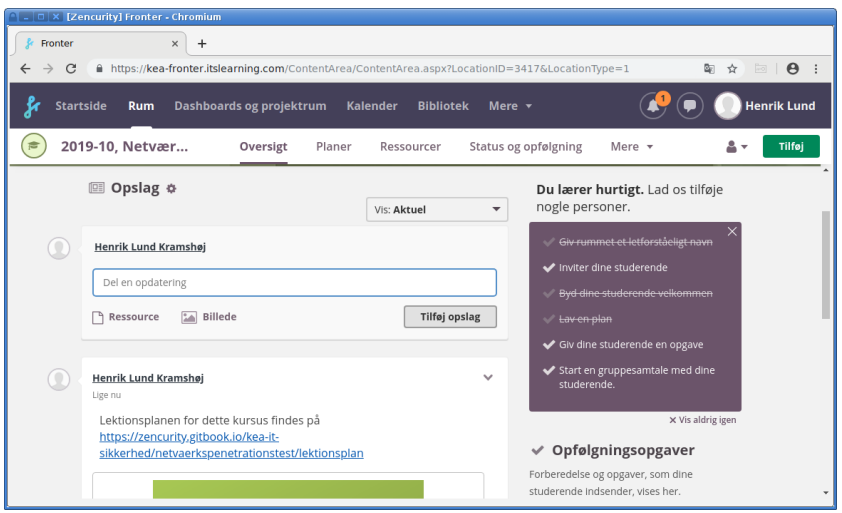
Bemærk: kursusmaterialet er ikke en substitut for andet materiale, der er udeladt mange detaljer som forklares undervejs, eller kan slås op op internet

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 go to the exam.

Fronter Platform



KEA use fronter for sharing news during the course:
`https://kea-fronter.itslearning.com/`

I use the following link:
`https://zencurity.gitbook.io/kea-it-sikkerhed/netvaerkspenetrationstest/lektionsplan`

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018

Indhold:
Den studerende lærer om hvordan en penetration test udføres, samt kan indhente oplysninger om de seneste sårbarheder, og kan benytte sig af de relevante værktøjer til dette formål.

Viden
Den studerende viden om og forståelse for:

- Etiske samt kontraktuelle forhold omkring en penetrationstest.
- Standardiseringorganisationers og myndigheders krav til og om penetrationstesting

Færdigheder
Tage højde for sikkerhedsaspekter ved at:

- Anvende relevante metoder ved udførsel af en penetrationstest
- Udarbejde en angrebsplan ud fra indsamlede oplysninger om et mål
- Finde sårbarheder i et givet system
- Dokumentere og rapportere fundne sårbarheder

Kompetencer Den studerende kan:

- Planlægge en penetration test, samt eksekvere den både ved brug af værktøjer og manuelt

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

Forudsætninger

Dette er en workshop og fuldt udbytte kræver at deltagerne udfører praktiske øvelser

Kurset anvender Kali Linux til øvelser, men UNIX kendskab er ikke nødvendigt

Øvelserne foregår via virtuel maskine

- Til penetrationstest og det meste Internet-sikkerhedsarbejde er der følgende forudsætninger
- Netværkserfaring
- TCP/IP principper - ofte i detaljer
- Programmmeringserfaring er en fordel
- UNIX kendskab er ofte en **nødvendighed**
  - fordi de nyeste værktøjer er skrevet til UNIX i form af Linux og BSD

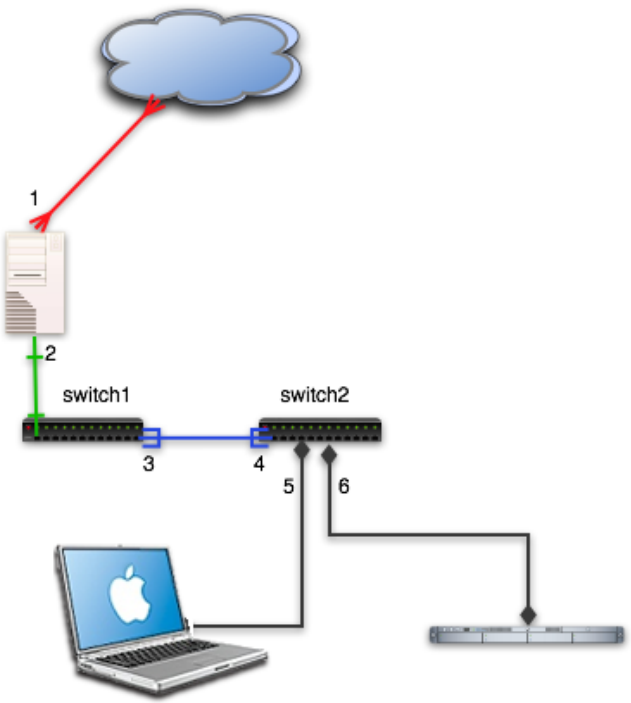
Kursusfaciliteter

.

KEA har et trådløst netværk, som kan bruges til de fleste ting

Til visse opgaver medbringer jeg et kursusnetværk med:

- Router
- Switch
- Wi-Fi Access Point

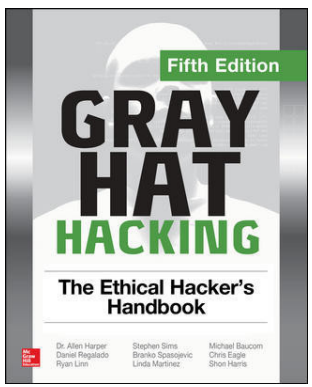


Primary literature

Primary literature are these books:

- *Gray Hat Hacking: The Ethical Hacker's Handbook*, fifth edition Allen Harper and others ISBN: 978-1-260-10841-5, May 2018, 640 pp.- shortened grayhat
- *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: Gray Hat Hacking (Grayhat)

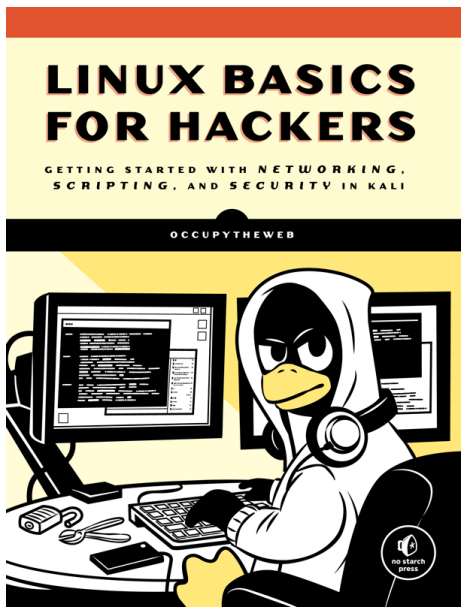


Gray Hat Hacking: The Ethical Hacker's Handbook, fifth edition

Authors: Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, Shon Harris
Published: May 18th 2018 Paperback ISBN: 978-1-260-10841-5 640 pp.

`https://www.mhprofessional.com/9781260108415-usa-gray-hat-hacking-the-ethical-hackers-handbook-fifth-edition-group`

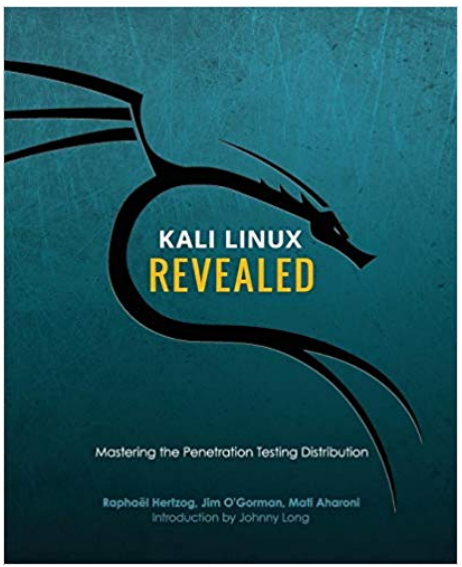
Book: Linux Basics for Hackers (LBhF)



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`

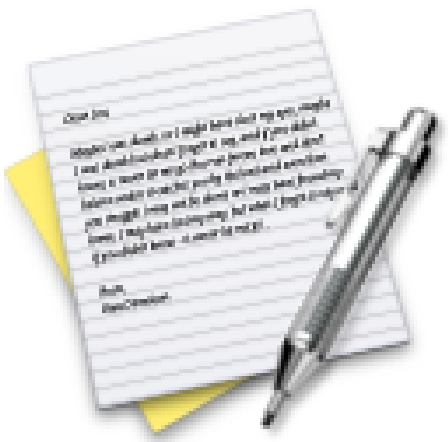
Book: Kali Linux Revealed (KLR)



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

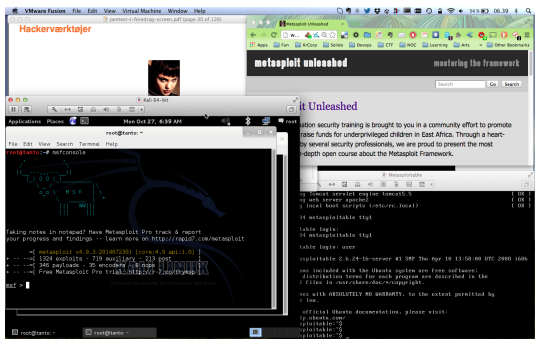


Now lets do the exercise

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 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.

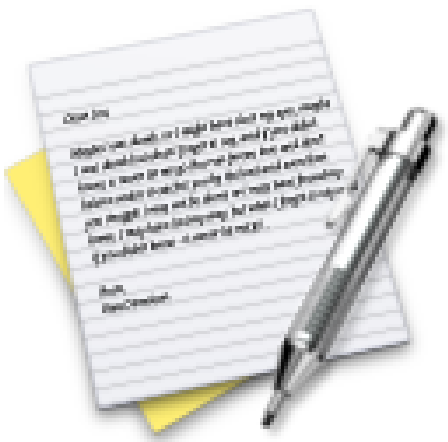
Aftale om test af netværk

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

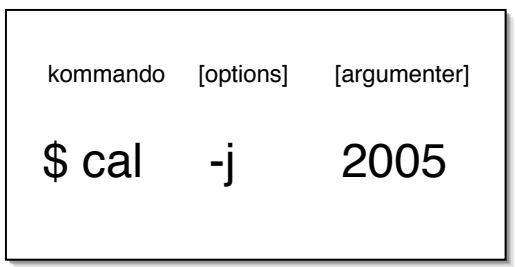
Check your Kali VM, run Kali Linux 30 min

which is number 2 in the exercise PDF.

Lab setup and Nmap Workshop

- We will now do two things:
- Prepare/finish your lab setup
  `https://github.com/kramse/kramse-labs`
- Switch to the materials found in my Nmap Workshop and perform some Nmap scans
  `https://github.com/kramse/security-courses/tree/master/courses/pentest/nmap-workshop`

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

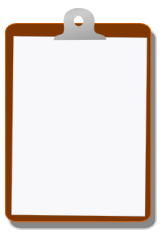
Adgang til UNIX kan ske via grafiske brugergrænseflader, eksempelvis

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

eller kommandolinien

Jeg anbefaler XFCE, som også er default på Kali pt. og findes til Debian

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!