

Penetration Testing exercises

Henrik Lund Kramshoej
hlk@zencurity.com

November 5, 2019



Contents

1	Download Kali Linux Revealed (KLR) Book 10 min	3
2	Check your Kali VM, run Kali Linux 30 min	4
3	Try a system for writing pentest reports 30 min	5

Preface

This material is prepared for use in *Communication and Network Security workshop* and was prepared by Henrik Lund Kramshøj, <http://www.zencurity.com> . It describes the networking setup and applications for trainings and workshops where hands-on exercises are needed.

Further a presentation is used which is available as PDF from kramse@Github
Look for kea-pentest-exercises in the repo security-courses.

These exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of tools which can be copied and reused after training. A lot is described about setting up your workstation in the repo

<https://github.com/kramse/kramse-labs>

Prerequisites

This material expects that participants have a working knowledge of TCP/IP from a user perspective. Basic concepts such as web site addresses and email should be known as well as IP-addresses and common protocols like DHCP.

Have fun and learn

Introduction to networking

IP - Internet protocol suite

It is extremely important to have a working knowledge about IP to implement secure and robust infrastructures. Knowing about the alternatives while doing implementation will allow the selection of the best features.

ISO/OSI reference model

A very famous model used for describing networking is the ISO/OSI model of networking which describes layering of network protocols in stacks.

This model divides the problem of communicating into layers which can then solve the problem as smaller individual problems and the solution later combined to provide networking.

Having layering has proven also in real life to be helpful, for instance replacing older hardware technologies with new and more efficient technologies without changing the upper layers.

In the picture the OSI reference model is shown along side with the Internet Protocol suite model which can also be considered to have different layers.

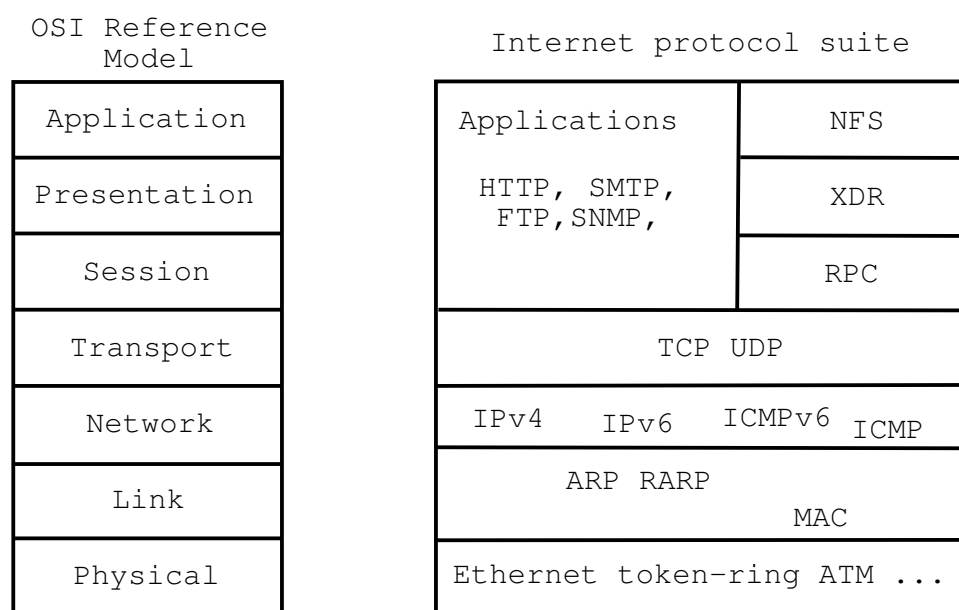


Figure 1: OSI og Internet Protocol suite

Exercise content

Most exercises follow the same procedure and has the following content:

- **Objective:** What is the exercise about, the objective
- **Purpose:** What is to be the expected outcome and goal of doing this exercise
- **Suggested method:** suggest a way to get started
- **Hints:** one or more hints and tips or even description how to do the actual exercises
- **Solution:** one possible solution is specified
- **Discussion:** Further things to note about the exercises, things to remember and discuss

Please note that the method and contents are similar to real life scenarios and does not detail every step of doing the exercises. Entering commands directly from a book only teaches typing, while the exercises are designed to help you become able to learn and actually research solutions.

Exercise 1

Download Kali Linux Revealed (KLR) Book 10 min



Kali Linux Revealed Mastering the Penetration Testing Distribution

Objective:

We need a Kali Linux for running tools during the course. This is open source, and the developers have released a whole book about running Kali Linux.

This is named Kali Linux Revealed (KLR)

Purpose:

We need to install Kali Linux in a few moments, so better have the instructions ready.

Suggested method:

Create folders for educational materials. Go to <https://www.kali.org/download-kali-linux-revealed-book/> Read and follow the instructions for downloading the book.

Solution:

When you have a directory structure for download for this course, and the book KLR in PDF you are done.

Discussion:

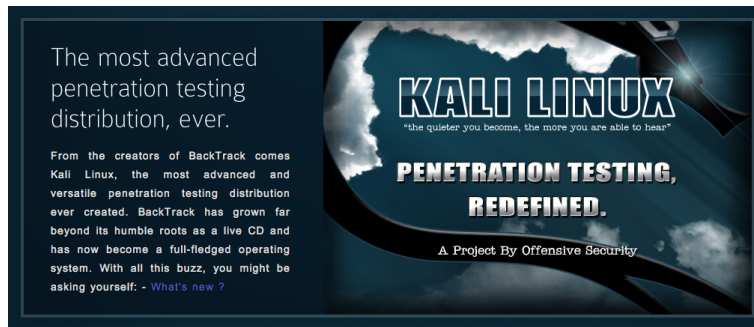
Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux is a free pentesting platform, and probably worth more than \$10.000

The book KLR is free, but you can buy/donate, and I recommend it.

Exercise 2

Check your Kali VM, run Kali Linux 30 min



Objective:

Make sure your virtual machine is in working order.

We need a Kali Linux for running tools during the course.

Purpose:

If your VM is not installed and updated we will run into trouble later.

Suggested method:

Go to <https://github.com/kramse/kramse-labs/>

Read the instructions for the setup of a Kali VM.

Hints:

If you allocate enough memory and disk you won't have problems.

Solution:

When you have a updated virtualisation software and Kali Linux, then we are good.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux includes many hacker tools and should be known by anyone working in infosec.

Exercise 3

Try a system for writing pentest reports 30 min

$\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ is fun!

Objective:

Try creating a pentest report!

Purpose:

We will do a handin requiring you to do a pentest report! So why not look at an example report and system for creating this.

Suggested method:

Go to <https://github.com/kramse/pentest-report>

Read the instructions for the setup of Kali with TeXlive - a $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ system.

Hints:

$\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$ is not the only system that can be used, but one I prefer over wysiwyg text processing. It can be automated!

Also you can add scripts and include results and files directly into the report!

Solution:

When you have looked at the repo you are done, you dont need to work with this system - its optional.

Discussion:

Another template is from the Offensive Security OSCP program.

<https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>

and this one suggested by Jack

<https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>