Computer Systems Security exercises

Henrik Lund Kramshoej
hlk@zencurity.com

April 16, 2019

Contents

Preface

This material is prepared for use in *Computer Systems Security workshop* and was prepared by Henrik Lund Kramshoej, 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 system-security-exercisesin 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 expect 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

Exercise content

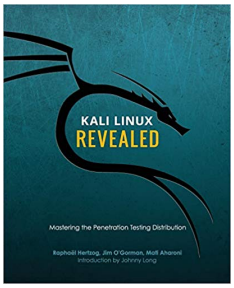
Most exercises follow the same procedure and has the following content:

- **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 wont 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

Check your Debian VM 10 min

Objective:
Make sure your virtual Debian 9 machine is in working order.

We need a Debian 9 Linux for running a few extra tools during the course.

This is a bonus exercise - one is needed per team that want to try these tools. Tools which need Debian are Zeek and Suricata.

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:

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.

Exercise 4

Risk Assessment 101

> In quantitative risk assessment an annualized loss expectancy (ALE) may be used to justify the cost of implementing countermeasures to protect an asset. This may be calculated by multiplying the single loss expectancy (SLE), which is the loss of value based on a single security incident, with the annualized rate of occurrence (ARO), which is an estimate of how often a threat would be successful in exploiting a vulnerability.

Quote from https://en.wikipedia.org/wiki/Risk_assessment

Objective:
Do calculations to understand risk assessment better

Purpose:

Suggested method:

Hints:

Solution:

Discussion:
What we have done here is Quantitative Risk Assessment.

Other risk analysis methods exist, qualitative risk analysis - used when it is difficult to put amount

Exercise 5

Run Armitage - Hail Mary

Objective:
Try hacking using a graphical program, see how quick and easy it can be.

Purpose:
Show that when a vulnerability exist attacks can be quick and easy.

Suggested method:

1. Boot up Kali Linux
2. Boot up Metasploitable - from ISO
3. Run Armitage Hail-Mary against Metasploitable
4. Note which succeeded, describe those attacks that succeeded in relation to MITRE ATT&CK framework

Hints:

Solution:

Discussion:

Exercise 6

SELinux Introduction

Objective:

Purpose:

Suggested method:
Try enabling and disabling the policies

Hints:

Solution:

Discussion:

Exercise 7

Example AUPs

Objective:
See real world high level policies

Purpose:

Suggested method:
Find your AUP for the ISPs we use, you use, your company uses

Hints:

Solution:

Discussion:

Exercise 8

Database Security

Objective:

Purpose:

Suggested method:

Hints:

Solution:

Discussion:
Databases - discussion about Relational Database Management System RDBMS Model and NoSQL

Exercise 9

SYN flooding 101

Objective:

Purpose:

Suggested method:

Hints:

Solution:

Discussion:

Exercise 10

Medical Security Oolicies

Objective:

Purpose:

Suggested method:
Find example medical security policies

Fitbit

Hints:

Solution:

Discussion:

Exercises

Exercise 11

Perform privilege escalation using files

Objective:
Perform a simple privilege escalation attack

Purpose:

Suggested method:

1. Make a non-privileged user
2. make a system directory writable
3. create root cronjob without path
4. Insert a malicious script as one of the commands from the root cron job

Hints:
A cron job runs scheduled commands. They usually perform cleanup functions, removing old files, doing a backup or similar

Solution:

Discussion:
This was chosen as I found a similar vulnerability in a professional product, in 2019

Exercise 12

Anti-virus and ”endpoint security”

Objective:
Discuss when to use Anti-virus and ”endpoint security”

Purpose:

Suggested method:

Hints:

Solution:

Discussion:

