Sikker browsing, plugins og Tor project workshop

Henrik Lund Kramshoej
hlk@zencurity.com

April 5, 2019

Contents

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Preface

This material is prepared for use in *Sikker browsing, plugins og Tor project 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 crypto-party-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

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

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.

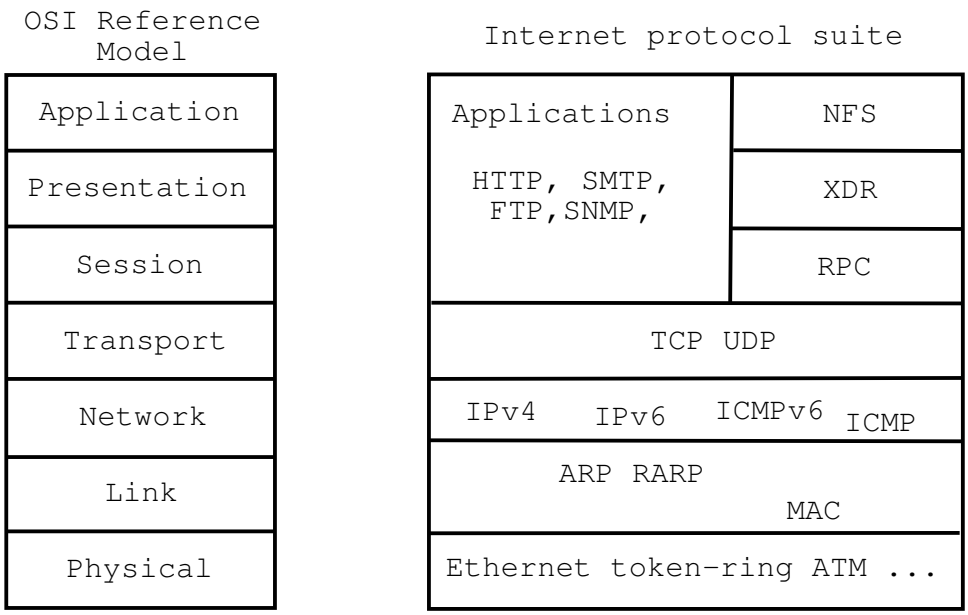

Figure 1: OSI og Internet Protocol suite

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

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.

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 1

Installation af alternativ browser

Objective:
Installer en alternativ browser på din PC, eksempelvis Firefox eller Chrome
Suggested method:
Hent installationsprogrammet fra http://www.mozilla.org eller http://www.google.com/chrome
En ekstra browser giver mulighed for nemt at have sikre indstillinger når man surfer på internet.
Solution:
Hent installationsprogrammet og udfør installationen
Discussion:
Vi bruger Firefox for at have en alternativ browser, som kan indstilles mere paranoidt, kan udvides med plugins, Flash blocker m.v.
Det er valgfrit hvilken browser man vælger, men en alternativ browser giver muligheder for bedre sikkerhedsindstillinger.
Mac brugere kan derefter bruge Safari, mens Windows brugere kan fortsætte med Internet Explorer til NemID/Netbank og sites man stoler på.
Husk at installere plugins som:

- Firefox CertPatrol
- Firefox / Chrome - HTTPS Everywhere
- Firefox NoScripts/ Chrome NotScripts

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 2

Installation af Torbrowser

Objective:
Installer Torbrowser pakken fra http://www.torproject.org/
Suggested method:
Hent installationsprogrammet og installer
Suggested method:

Solution:

Discussion:

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 3

Installation af Thunderbird mail program

Objective:
Installer Thunderbird mailklienten på din PC
Suggested method:
Hent installationsprogrammet lokalt eller fra http://www.mozilla.org
Suggested method:

Solution:
Hent installationsprogrammet og udfør installationen.
Discussion:
Thunderbird anbefales fremfor eksempelvis Outlook og Apple Mail grundet de gode muligheder for udvidelser, herunder Enigmail OpenGPG plugin.
på Mac OS X kan benyttes den indbyggede Mail.app med GPGMail plugin - hvis man kan leve med at den ikke altid findes til nyeste version af Mac OS X.
på andre UNIX varianter er Mutt mail reader populær og integrerer nemt til OpenGPG.
Thunderbird giver også mulighed for nem mail filtrering med eksempelvis Sieve og Dovecot.

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 4

Installation af GPG GNU Privacy Guard

Objective:
Installer GNU Privacy Guard på jeres PC.
Suggested method:
Hent installationsprogrammet og installer - brug pakkesystemerne hvis I bruger Linux
Mac OS X brugere kan med fordel benytte https://www.gpgtools.org/
Suggested method:

Solution:

Discussion:

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 5

Installation af Enigmail plugin

Objective:
Installer Enigmail plugin til Thunderbird
Suggested method:
Hent installationsprogrammet og installer
Suggested method:

Solution:
Det nemmeste er at gå til hjemmesiden for Enigmail
http://enigmail.mozdev.org/
Discussion:
Enigmail kræver at GNU Privacy Guard er installeret

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 6

Lav en PGP-kompatibel nøgle

Objective:
Brug et valgfrit program til at lave en PGP-kompatibel nøgle
Forslag til fremgangsmåde:
Brug Enigmail Key Manager eller PGP pakken til at generere en nøgle
Hjælp:
Sørg for at lave din første nøgle med udløbsdato!
Sørg for at lave et revocation certificate på din første nøgle - så kan du altid trøkke den tilbage - selvom du glemmer kodeordet.
Forslag til løsning:
Brug det lokale mailsetup som eksempel og lav en nøgle
Discussion:
Husk at hvis det skal være en rigtig nøgle skal du helst bruge din rigtige mailadresse
Jeg vil ikke anbefale at der uploades "testnøgler" til keyservere, da man ikke kan slette sine nøgler.

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 7

Hent en nøgle fra en anden

Objective:
Find en nøgle og indlæs den i din nøglering
Suggested method:
Brug enten en keyserver http://pgp.mit.edu eller en USB nøgle til at overføre en elektronisk udgave af nøglen til din PC
husk at verificere fingerprint
Suggested method:

Solution:

Discussion:

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 8

Send en krypteret mail

Objective:
Send en krypteret mail
Suggested method:
Brug PGP pakken eller Thunderbird til at sende en krypteret mail til en af de andre
Suggested method:

Solution:

Discussion:

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 9

Signer en nøgle

Objective:
Find ud af hvordan du laver en signatur på en nøgle og returnerer den
Suggested method:

Suggested method:

Solution:

Discussion:
Det er en god politik KUN at signere nøgler hvor man har fået fremvist officielle papirer som kørekort og pas.
Læg yderligere mærke til at det som signaturen angiver er om den nøgle tilhører vedkommende - ikke om vedkommende er troværdig!

© license CC BY 3.0. 2019 Henrik Lund Kramshøj

Exercise 10

Installation af FileZilla

Objective:
Installer FileZilla pakken fra http://filezilla-project.org/
Suggested method:
Hent installationsprogrammet og installer FileZilla, alternativt WinSCP eller et andet program der forstår SFTP
Suggested method:

Solution:

Discussion:
Det er vigtigt at bruge sikre protokoller når man overfører data, eksempelvis til opdatering af websites

© license CC BY 3.0. 2019 Henrik Lund Kramshøj