Welcome to

8. Secure Systems Design and Implementation

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

8-secure-systems-design.tex in the repo security-courses

Plan for today

Subjects

- Principle of least privilege, fail-safe defaults, separation of privilege etc.
- Files, objects, users, groups and roles
- Naming and Certificates
- Access Control Lists
- DNSSEC

Exercises

- DNSSEC, SPF, DMARC - DNS based updates to your email domain security

Reading Summary

Bishop chapter 14: Design Principles

Bishop chapter 15: Representing Identity

Bishop chapter 16: Access Control Mechanisms

Skim, Setuid demystified

Some thoughts on security after ten years of qmail 1.0

Wedge: Splitting Applications into Reduced-Privilege Compartments

Principle of least privilege, fail-safe defaults, separation of privilege etc.

Files, objects, users, groups and roles

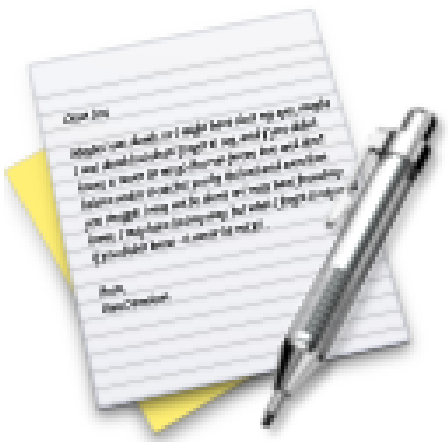
Naming and Certificates

Access Control Lists

DNSSEC

Hardenize - web site with testing

Exercise

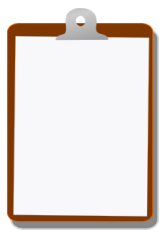


Now lets do the exercise

??

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

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 less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools