Welcome to

# 6. Malware, Intrusion, Vulnerabilities

## KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

6-malware-intrusion-vulnerabilities.tex in the repo security-courses

# Plan for today

## Subjects

- Trojan horses, Rootkits, computer viruses
- Computer worms, from Morris Worm to today
- Bots and botnets
- Ransomware
- Phishing and spear phishing
- Sandboxing, Java and browsers
- Penetration testing
- Common Vulnerabilities and Exposure CVE
- Common Weaknesses and Exposures CWE

## Exercises

-
-

# Reading Summary

Bishop chapter 23: Malware

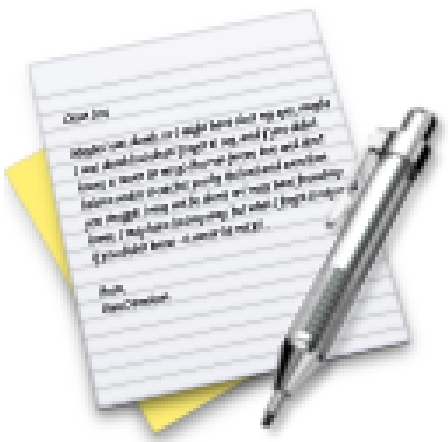
Bishop chapter 24: Vulnerability Analysis

Smashing The Stack For Fun And Profit, Bypassing non-executable-stack during exploitation using return-to-libc, Basic Integer Overflows, Return-Oriented Programming

# Trojan horses, Rootkits, computer viruses

# Computer worms, from Morris Worm to today

# Exercise



Now lets do the exercise

## Perform privilege escalation using files

which is number **11** in the exercise PDF.

# Bots and botnets

# Ransomware

# Phishing and spear phishing

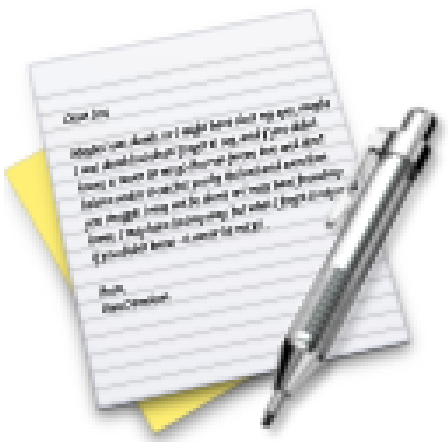
# Sandboxing, Java and browsers

# Penetration testing

# Common Vulnerabilities and Exposure CVE

# Common Weaknesses and Exposures CWE

# Exercise

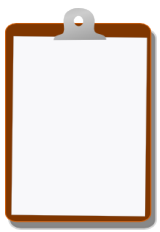


Now lets do the exercise

## Anti-virus and ”endpoint security”

which is number **12** 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