



Welcome to

## 11. Forensics 2: Incident Response

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse  

Slides are available as PDF, kramse@Github  
11-forensics-incident-response.tex in the repo security-courses

# Plan for today



## Subjects

- Attack and Response
- Attack graphs
- Attack surfaces, and reducing them
- Intrusion Handling, phases

## Exercises

- Clean or rebuild a server
- Cloud environments influence on incident response

# Reading Summary



Browse

and read this

Browse / skim this:

# Attack and Response



# Attack graphs



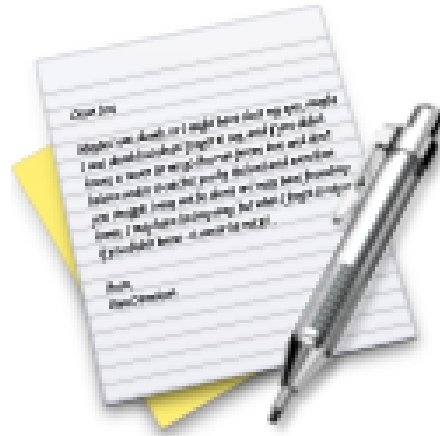
# Attack surfaces, and reducing them



# Intrusion Handling, phases



# Exercise



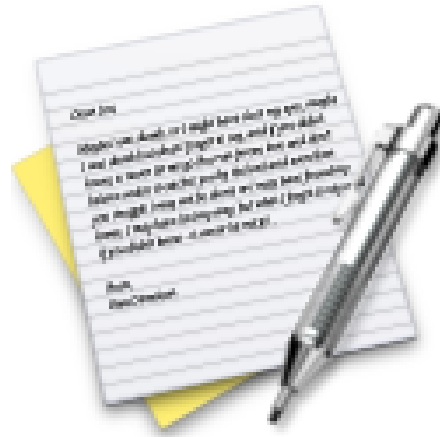
Now lets do the exercise

## Clean or rebuild a server

which is number **21** in the exercise PDF.



# Exercise

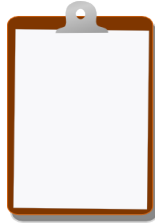


Now lets do the exercise

## Cloud environments influence on incident response

which is number **22** 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