Welcome to

10. Forensics 1: Auditing and Intrusion Detection

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

10-forensics-auditing-intrusions.tex in the repo security-courses

Plan for today

Subjects

- Auditing and logging
- Volatility and file systems
- Intrusion Detection
- Host and Networks Based Intrusion Detection (HIDS/NIDS)
- Network Security Monitoring

Exercises

- Centralized syslogging and example system
- Open a file system dump

Reading Summary

Bishop chapter 25: Auditing

Bishop chapter 26: Intrusion Detection

And at least 27.4 - or chapter 27 too

Download and browse the ENISA papers listed under Computer Forensics in the reading list

Auditing and logging

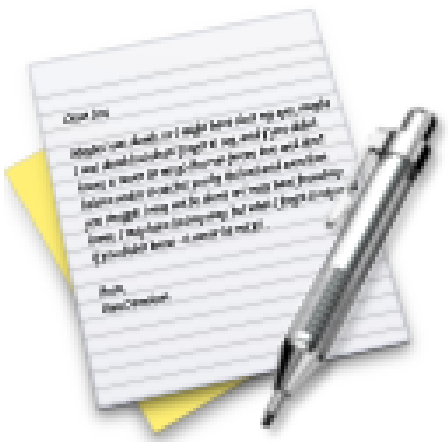
Volatility and file systems

Intrusion Detection

Host and Networks Based Intrusion Detection (HIDS/NIDS)

Network Security Monitoring

Exercise

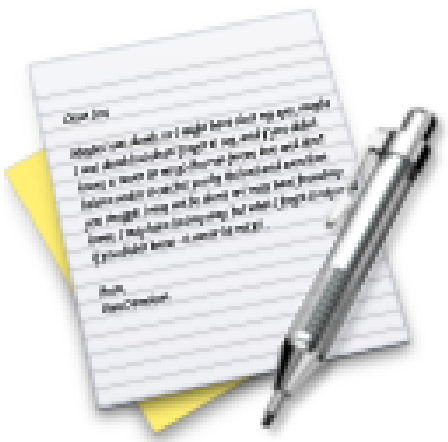


Now lets do the exercise

Centralized syslog

which is number **19** in the exercise PDF.

Exercise

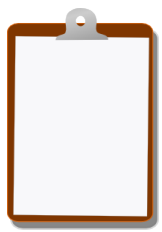


Now lets do the exercise

File System Forensics

which is number **20** 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