Kickstart: Introduction to Incident Response elective course

This material is prepared for use in *Introduction to Incident Response elective course* and was prepared by Henrik Kramselund, `xhek@kea.dk`. It contains the very basic information to get started!

These course and 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 Github repositories.

To get kickstarted in this course:

□ Make sure you can login to Fronter https://kea-fronter.itslearning.com/
Electronic version of this document will be uploaded here!

□ Lecture plan for this course will be in Fronter
(Source is also in Git https://github.com/kramse/kea-it-sikkerhed)

□ Bookmark the main Github page: https://github.com/kramse/
Note: there are two pinned repositories `security-courses` and `kramse-labs`

□ Slides and exercises booklet – PDF will be in Fronter
Source is in Github – feel free to clone or download single files
https://github.com/kramse/security-courses/tree/master/courses/incident-response/incident-response

□ Get the book *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781491934944

□ Get the book *Forensic Discovery* (FD), Dan Farmer and Wietse Venema! You can download *for free*: http://fish2.com/security/

□ Get the document *Computer Security Incident Handling Guide*, NIST SP 800-61 Rev. 2, August 2012 https://doi.org/10.6028/NIST.SP.800-61r2

□ Create a Debian Linux VM version 12 Bookworm – it is enough if each group has one Debian VM

I hope we will have a fun and enjoyable time in this course.

Best regards

Henrik Kramselund, he/him