description: Elective Course Introduction to Incident Response (5 ECTS)

Lecture planning

Course: Introduction to Incident Response (5 ECTS)

General Information

Teacher: Henrik Kramselund xhek@kea.dk hlk@zencurity.dk +45 2026 6000

This document is written using Github.

Teaching material will primarily be English, but the teaching will be in Danish.

Goals

The module is an introduction to Incident Response that will describe the basics of incident response. This will include the terms, tools and processes used by professionals.

See more about the course in the official curriculum.

Exam:

Date: TBD exam date

Teaching Methods:

- Lecture lessons
- Group exercises and cases, including practical exercises with laptop

Teaching dates - Spring 2024:

Teaching dates: thursdays 12:45 - 16:00 in GBG.E512

1/2, 8/2, 9/2, 15/2, 22/2, 29/2, 14/3, 11/4

The date 7/3 will need to be changed, I am at a conference. Probably it will be a mandatory assignment this day.

New date will be added, perhaps 26/3 or 26/3 to replace 21/3

Hardware

Since we are going to be doing exercises, each team will need laptops.

Read more about these at https://github.com/kramse/kramse-labs

Course reading list

This course uses a few books and a number of supporting resources.

Primary literature:

- *Intelligence-Driven Incident Response* (IDIR),
  Scott Roberts, Rebekah Brown, ISBN: 9781098120689 **2nd edition 2023** - short IDIR

- *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages. This book is currently available for ”free” via: http://fish2.com/security/
  but recommend buying it.

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

It is recommended to get these books. Note: we won't read all chapters and pages.

Also the course will use internet links and pages.

Supporting Internet resources

- The Linux Command Line: A Complete Introduction, 2nd Edition, William Shotts
  Download -- internet edition https://sourceforge.net/projects/linuxcommand
- Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7
- The Debian Administrator’s Handbook, Raphaël Hertzog and Roland Mas
  https://debian-handbook.info/ - shortened DEB
- Kali Linux Revealed Mastering the Penetration Testing Distribution https://www.kali.org/download-kali-linux-revealed-book/ - shortened KLR
- The JavaScript Object Notation (JSON) Data Interchange Format RFC8259
  https://tools.ietf.org/html/rfc8259
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D.
  Lockheed Martin Corporation
  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
- The Diamond Model of Intrusion Analysis, Sergio Caltagirone, Andrew Pendergast, Christopher Betz
  http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- Development of a virtualized security operations center, Robert de Céspedes, George Dimitoglou
  https://dl.acm.org/doi/abs/10.5555/3512489.3512501

Other relevant papers and documents can often be found in the NIST publications, Special Publications series 800:
https://csrc.nist.gov/publications/sp800

Example the Guide to Computer Security Log Management SP800-92

Attacks on infrastructure:

- Smashing The Stack For Fun And Profit, Aleph One
- *An Evening with Berferd: In Which a Cracker is Lured, Endured, and Studied* , Bill Cheswick, AT&T Bell Laboratories
  http://www.cheswick.com/ches/papers/berferd.pdf
- Return-Oriented Programming:Systems, Languages, and Applications
  Ryan Roemer, Erik Buchanan, Hovav Shacam and Stefan Savage University of California, San Diego
- MITRE ATT&CK a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, read the ATT&CK 101 Blog Post
- Enterprise Survival Guide for Ransomware Attacks, Shafqat Mehmoon, SANS Information Securiy Reading Room
- TCP Synfloods - an old yet current problem, and improving pf's response to it
  Henning Brauer, BSDCan 2017
- *A Graduate Course in Applied Cryptography* By Dan Boneh and Victor Shoup https://toc.cryptobook.us/
  https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf

Computer Forensics, Incident Response, Intrusion Detection

- Incident Handler's Handbook
  by Patrick Kral, SANS Information Security Reading Room
- An Intrusion-Detection Model, Dorothy E. Denning
  IEEE Transactions on Software Engineering (Volume: SE-13 , Issue: 2 , Feb. 1987)
- ENISA Presenting, correlating and filtering various feeds Handbook, Document for teachers
  https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/presenting-correlating-and-filtering-various-feeds-handbook
- ENISA Forensic analysis, Network Incident Response https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2_forensic_analysis_ii-handbook
- ENISA Network Forensics, Handbook, Document for teachers https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/network-forensics-handbook

Policies, governance and best Practice

- Campus Network Security: High Level Overview , Network Startup Resource Center
- Campus Operations Best Current Practice, Network Startup Resource Center
- CIS Controls Requires giving your email
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management
- IT Security Guidelines for Transport Layer Security (TLS)

Planning

The detailed plan is below with a table summarizing lessons

Date	Theme	Description	Litterature / Preparation
1/2	**0. Getting Started**	Welcome, goals and expectations Prepare Tools - bring laptop. Get the books Find some basic logs on your computers, introduce incidents and some statistics	Get the books. Chapters IDIR 1-2 will be discussed
8/2 AND 9/2	**1. Basics of Incident Response**	Incident Response Cycle, Kill Chain, Mitre ATT&CK	Chapters IDIR 3
15/2	**2. Find, Fix, F3EAD started**	F3EAD and exploit phases - artifacts found	Chapters IDIR 4-5
22/2	**3. Mitigate and Monitor**	Mitigate, Remediate, Monitoring LifeCycle	Chapters IDIR 6
29/2	**4. Structured Incident Response and IoCs**	Going from Indicators of Compromise into escalating and handling incidents	Chapters IDIR 7
7/3 - to be changed	**5. Malware and Incident Response**	Malware in relation to Incident Response. Ransomware, some basic analysis and tools	Chapters IDIR 8

Date	Theme	Description	Litterature / Preparation
14/3	**6. Reporting on Incident Response**	Collecting and disseminate results from incidents	Chapters IDIR 9
21/3 - to be moved!	**7. Threat Hunting and Intelligence**	Basic Threat Hunting and how to share threat intelligence	
11/4	**8. The Way Forward: Building an Intelligence Program**	Describe the process for implementing an efficient incident response in an organisation	Chapters IDIR 10-11