description: Valgfrie modul VF1 Systemsikkerhed (10 ECTS) System Security

Lektionsplan

Fagets titel: VF1 Systemsikkerhed (10 ECTS)

General Information

English: Computer Systems Security

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

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

Goals

The module is centered around the design and implementation of secure computer systems.
Topics include operating system (OS) security, capabilities, and more.

See more about the course in the official curriculum.

Exam:

Date: April 3rd, 2025

Teaching Methods:

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

Teaching dates: tuesdays and thursdays 17:00 - 20:30

The dates are for 2025:
28/1, 30/1, 4/2, 6/2, 11/2, 13/2, 18/2, 20/2, 25/2, 27/2, 4/3, (6/3 moved), 11/3, 13/3, 18/3

The date 6/3 was moved to 18/3 instead.

Course reading list

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

Primary literature:

- *Defensive Security Handbook* (DSH), 2nd Edition
  by Lee Brotherston, Amanda Berlin, William F. Reyor, June 2024, O'Reilly Media, Inc.
  ISBN: 978-1-098-127244
- *Windows 11 Security Book: Powerful security by design* (MSFT), Microsoft 2023, short 80 page PDF
  https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MSFT-Windows11-Security-book_Sept2023.pdf

- *Mastering Linux Security and Hardening* (MLSH), third edition, Donald A. Tevault, 2023 ISBN: 9781837630516 https://www.packtpub.com/product/mastering-linux-security-and-hardening-third-edition/9781837630516

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

Supporting literature - optional, but recommended:

- *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages. Can be found at http://www.porcupine.org/forensics/forensic-discovery/ but recommend buying it
- *The Linux Command Line: A Complete Introduction*, 2nd Edition by William Shotts Print: https://nostarch.com/tlcl2 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 - shortened LBfH

Also the course will use internet links and pages.

Supporting Internet resources

- The Debian Administrator’s Handbook, Raphaël Hertzog and Roland Mas https://debian-handbook.info/ - shortened DEB
- Kali Linux Revealed Mastering the Penetration Testing Distribution - shortened KLR

Control Hijacking Attacks

- Smashing The Stack For Fun And Profit, Aleph One
- Bypassing non-executable-stack during exploitation using return-to-libc
by c0ntex.
- Basic Integer Overflows by blexim.
- 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

OS Security

- Secure Programming for Linux and Unix HOWTO), David Wheeler.
- Setuid demystified by Hao Chen, David Wagner, and Drew Dean.
- Some thoughts on security after ten years of qmail 1.0 Daniel J. Bernstein.
- Wedge: Splitting Applications into Reduced-Privilege Compartments by Andrea Bittau, Petr Marchenko, Mark Handley, and Brad Karp.
- Capsicum: practical capabilities for UNIX Robert N. M. Watson University of Cambridge, Jonathan Anderson University of Cambridge, Ben Laurie Google UK Ltd., Kris Kennaway Google UK Ltd.
- Removing ROP Gadgets from OpenBSD Todd Mortimer mortimer@openbsd.org
- TCP Synfloods - an old yet current problem, and improving pf's response to it
Henning Brauer, BSDCan 2017

Exploiting Hardware Bugs and Crypto Related

- Bug Attacks on RSA, by Eli Biham, Yaniv Carmeli, and Adi Shamir.
- Using Memory Errors to Attack a Virtual Machine by Sudhakar Govindavajhala and Andrew Appel
- Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu, see also Exploiting the DRAM rowhammer bug to gain kernel privileges
- *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

- 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
- 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)
- Forensic Discovery Dan Farmer, Wietse Venema, Addison-Wesley Professional, 2005

Policies, governance and best Practice

- Campus Network Security: High Level Overview , Network Startup Resource Center
- Campus Operations Best Current Practice, Network Startup Resource Center
- Mutually Agreed Norms for Routing Security (MANRS)
- 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	Litterature / Preparation
	Welcome and getting started	
28/1	Prepare Kali Linux VM - bring laptop	Reviewing the literature list will occur when we meet. Download PDF documents Create VMs
	Overview of Enterprise Attacks	
30/1	Overview of Computer Security	DSH chapters 1. Creating a Security Program, 2. Asset Management and Documentation MLSH ch 1
4/2	Enterprise Attacks	Read ATT&CK 101 Blog Post and browse MITRE ATT&CK MSFT Hardware Security and Operating System Security
6/2	User Accounts	MLSH 1-3 MSFT Identity, Privacy and Cloud Services
	Security Policies and Cryptography	

Date	Theme	Litterature / Preparation
11/2	Security Policies	DSH ch 3. Policies, 4. Standards and Procedures, 5. User Education, MLSH ch 4 - NOT firewalld part! Browse: Campus Network Security: High Level Overview , Network Startup Resource Center Campus Operations Best Current Practice, Network Startup Resource Center Mutually Agreed Norms for Routing Security (MANRS)
13/2	Basic Cryptography	MLSH ch 5, browse chapter 6 TLS1.2 RFC5246 table of contents - but only ToC, not the whole document! Skim: NIST Special Publication 800-63B Enterprise Survival Guide for Ransomware Attacks IT Security Guidelines for Transport Layer Security
	Securing the Architecture and Preventing Attacks	
18/2	Malware, Intrusion, Vulnerabilities	Skim: Forensics Discovery, ch 5-6 Browse: Smashing The Stack For Fun And Profit, Bypassing non-executable-stack during exploitation using return-to-libc, Basic Integer Overflows, Return-Oriented Programming MSFT Application Security
20/2	Secure Systems Design and Implementation	MLSH ch 7-8 Skim, Setuid demystified, Some thoughts on security after ten years of qmail 1.0, Wedge: Splitting Applications into Reduced-Privilege Compartments
25/2	Confinement and isolation	MLSH ch 9-10 Skim: Removing ROP Gadgets from OpenBSD
27/2	Breaking out	Read MLSH 11, DSH ch 18: Vulnerability Management Browse: Using Memory Errors to Attack a Virtual Machine paper, An Experimental Study of DRAM Disturbance Errors, Exploiting the DRAM rowhammer bug to gain kernel privileges https://en.wikipedia.org/wiki/Row_hammer
	Computer Forensic and Incident Response	
4/3	Auditing and Intrusion Detection	Read DSH ch 21: Understanding IDSs and IPSs, 22. Logging and Monitoring, MLSH 12 Skim: Forensics Discovery, ch 1-4 and appendix B Download and browse the ENISA papers listed under Computer Forensics in the reading list
11/3	Incident Response	Read DSH ch 6. Incident Response, 7. Disaster Recovery Browse: Incident Handler's Handbook
	System Security in Practice	

Date	Theme	Litterature / Preparation
13/3	Securing DNS and Email	DSH ch 23. The Extra Mile
18/3	Benchmarking and Auditing Recap	Read DSH ch 8. Industry Compliance Standards and Frameworks, skim ch 10-12: Windows, Unix and Endpoints CIS controls and PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019 MSFT Security Foundation and Conclusion, rest of the small book
	Prepare for the exam	Summary of the course, prepare for exam