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

This document is written using Github.

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: date coming for 2023 exam

Teaching Methods:

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

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

18/4, 20/4, 25/4, 27/2, 2/5, 4/5, 9/5, 11/5, 16/5, 30/5, 1/6, 6/6, 8/6, 13/6 2023

Course reading list

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

Primary literature:

- *Mastering Linux Security and Hardening* - Second Edition, Donald A. Tevault, 2020 ISBN: 9781838981778 - short MLSH
- *Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin ISBN: 978-1-491-96038-7 284 pages - short DSH
- *Forensics Discovery*, Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages. Can be found at http://www.porcupine.org/forensics/forensic-discovery/ but recommend buying it - short FD

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

Supporting literature - optional to buy, but recommended:

- *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
1/2	Welcome, goals and expectations Prepare Kali Linux VM - bring laptop	Reviewing the literature list will occur when we meet. Download PDF documents Create VMs
3/2	**Overview of Computer Security**	DSH chapters 1-2, MLSH ch 1
8/2	**Overview of Enterprise Attacks**	Read ATT&CK 101 Blog Post and browse MITRE ATT&CK
10/2	**User Accounts**	MLSH 1-2
15/2	**Security Policies**	DSH ch 3-5, MLSH ch 3-4 - 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)
17/2	**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

Date	Theme	Litterature / Preparation
22/2	**Malware, Intrusion, Vulnerabilities**	Browse: Smashing The Stack For Fun And Profit, Bypassing non-executable-stack during exploitation using return-to-libc, Basic Integer Overflows, Return-Oriented Programming
24/2	**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
1/3	**Capabilities**	MLSH ch 9-10 Skim: Removing ROP Gadgets from OpenBSD
3/3	**Breaking out**	Read DSH ch 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
8/3	**Forensics 1: Auditing and Intrusion Detection**	Read DSH ch 19-20, MLSH 12 Download and browse the ENISA papers listed under Computer Forensics in the reading list
10/3	**Forensics 2: Incident Response**	Read DSH ch 6-7 Browse: Incident Handler's Handbook
15/3	**System Security in Practice**	DSH ch 21
17/3	**Benchmarking and Auditing Recap**	Read MLSH 11, DSH ch 8, skim ch 10-12 CIS controls and PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
	Prepare for the exam	Summary of the course, prepare for exam