description: Obligatoriske modul Ob 1 Netværks- og kommunikationssikkerhed (10 ECTS) Communication and Network Security

Lektionsplan

Fagets titel: Ob 1 Netværks- og kommunikationssikkerhed (10 ECTS)

English: Communication and Network Security

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

This document is written using Github.

Goals

The module is centered around network threats and implementing and configuring equipment in this area.

Module includes different security equipment like IDS for monitoring.

The evaluation of security in a network, developing plans for closing security vulnerabilities in the network and a review of various VPN technologies.

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

See more about the course in the official curriculum.

Exam:

Date: 10/6 2024

Teaching Methods:

- Lecture lessons
- Group exercises and cases, including practical exercises with laptop
- 17:00 - 20:30 Hybrid physical and online meetup with exercises - planned!

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

2/4 2024, 9/4 2024, 11/4 2024, 16/4 2024, 18/4 2024, 23/4 2024, 25/4 2024, 30/4 2024, 2/5 2024, 7/5 2024, 14/5 2024, 16/5 2024, 21/5 2024, 23/5 2024

Course reading list

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

Primary literature:

- Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM

- Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems, 3rd edition 2017, Chris Sanders ISBN: 9781593278021 - shortened PPA

It is recommended to buy these books. The cost for all books will be about 1.000DKK

Curriculum will be chapters from the books, listed below!

Supporting literature is mostly background information, with a few exceptions. I do not expect you to read these in detail.

Supporting literature:

- *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 - especially if you dont know any Linux/Unix
- *Kali Linux Revealed Mastering the Penetration Testing Distribution* https://www.kali.org/download-kali-linux-revealed-book/ - shortened KLR
- *The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas can be downloaded from https://debian-handbook.info/
- *Security problems in the TCP/IP protocol suite*, S. M. Bellovin https://www.cs.columbia.edu/~smb/papers/ipext.pdf samt *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf
- *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
- *Firewalls and Internet Security: Repelling the Wily Hacker* , Second Edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin
  http://www.wilyhacker.com/ - shortened Cheswick
- *A Graduate Course in Applied Cryptography* By Dan Boneh and Victor Shoup https://toc.cryptobook.us/ Download latest version - currently version 0.5 https://toc.cryptobook.us/book.pdf
- *RFC5246 The Transport Layer Security (TLS)* https://tools.ietf.org/html/rfc5246
- *Strange Attractors and TCP/IP Sequence Number Analysis* , Michal Zalewski http://lcamtuf.coredump.cx/newtcp/
- *WireGuard: Next Generation Kernel Network Tunnel*, https://www.wireguard.com/papers/wireguard.pdf
- *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
- http://www.honeynet.org/sites/default/files/files/KYT-Picviz_v1_0.pdf
- *Campus Network Security: High Level Overview* , Network Startup Resource Center https://nsrc.org/workshops/2018/myren-nsrc-cndo/networking/cndo/en/presentations/Campus_Security_Overview.pdf
- *Campus Operations Best Current Practice*, Network Startup Resource Center https://nsrc.org/workshops/2018/tenet-nsrc-cndo/networking/cndo/en/presentations/Campus_Operations_BCP.pdf
- *Mutually Agreed Norms for Routing Security (MANRS)* https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf
- *RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks* https://tools.ietf.org/html/rfc2827

These can be downloaded from the internet for free and may be gathered by the instructor for easy download.

Also the course will use internet links and pages.

Hardware

Since we are going to be doing exercises, sniffing data it will be an advantage to have a wireless USB network card.

The following are two recommended models:

- TP-link TL-WN722N hardware version 2.0 cheap but only support 2.4GHz
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing

Both work great in Kali Linux for our purposes.

Unfortunately the vendors change models often enough that the above are hard to find. I recommend using your favourite search engine and research which cards work with Kali Linux and airodump-ng.

Planning

The detailed plan is below with a table summarizing lessons

Date	Theme	Goals	Litterature / Preparation
2/4	Welcome, goals and expectations Prepare Kali Linux VM - bring laptop	Create a good starting point for learning Introduce lecturer and students Concrete Expectations Prepare tools for the exercises	Reviewing the literature list will occur when we meet. Download Kali Linux Revealed Identification of chapters and sections from KLR and LBfH for reading as home assignment
9/4	**TCP/IP and Security in TCP/IP protocol suite**	Understand basic IP protocols and inherent security problems	Read: PPA chapters 1,2,3 - 52 pages, ANSM chapter 13 - 44 pages Skim: papers *Security problems in the TCP/IP protocol suite* and *A Look Back at "Security Problems ..."*
11/4	**Network Security Threats**	Know common threats in networks, and solutions	Read: PPA chapters 4,5,6 - 66 pages Skim: papers *Strange Attractors and TCP/IP Sequence Number Analysis*
16/4	**Traffic inspection and firewalls**	Understand basic firewall technologies	Read: ANSM chapter 1,2,3 - 73 pages https://en.wikipedia.org/wiki/Firewall_(computing) http://www.wilyhacker.com/ Cheswick chapter 2 og 3 PDF, ca 55 pages Skim: chapters from 1st edition: http://www.wilyhacker.com/1e/chap03.pdf http://www.wilyhacker.com/1e/chap04.pdf
18/4	**Encrypting the network**	Know how math, algorithms and protocols are used to ensure confidentiality and integrity	Read: PPA chapters 7,8,9 - 80 pages Skim: table of contents of RFC5246 The TLS Protocol Version 1.2 and the wikipedia page https://en.wikipedia.org/wiki/Transport_Layer_Security

Date	Theme	Goals	Litterature / Preparation
23/4	**Virtual Private Networks**	Know methods of connecting securely across insecure networks	Read: ANSM chapter 7,8 - 54 pages, https://en.wikipedia.org/wiki/Virtual_private_network https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104 IPSec VPN between JUNOS and Cisco IOS Skim: https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching https://en.wikipedia.org/wiki/OpenVPN https://en.wikipedia.org/wiki/IPsec https://en.wikipedia.org/wiki/DirectAccess https://www.wireguard.com/papers/wireguard.pdf
25/4	**Wifi Security**	Knowledge of Wireless 802.11 and security methods used	Read: PPA chapters 12, 13 - 60 pages Skim: http://aircrack-ng.org/doku.php?id=cracking_wpa
30/4	**Network Management**	Understand why managed networks are more secure	Read: PPA chapter 10,11 - 58 pages Skim: https://nsrc.org/workshops/2015/sanog25-nmm-tutorial/materials/snmp.pdf
2/5	**Network Intrusion Detection**	Learn how to sniff and detect network problems using IDS	Browse -- note a few headlines: ANSM chapter 9,10 - 86 pages - very usefull if you want to implement IDS. Not curriculum, but introduce IDS and are a good reference
7/5	**Network Forensics**	Introduction to network investigations	Read: ANSM chapter 4 - 24 pages Zeek documentation Intel framework https://docs.zeek.org/en/stable/frameworks/intel.html Suricata reputation support https://suricata.readthedocs.io/en/suricata-4.0.5/reputation/index.html
14/5	**Honeypots**	See how systems can attract attackers and monitor attacks	Read: ANSM chapter 12 Browse: ANSM chapter 11 - uses an older tool package SiLK but the process described is great
16/5	**DNS and Email Security**	Learn the role of DNS in securing networks and systems	Read: ANSM chapter 14,15 - 66 pages Re-Read: PPA DNS pages 173-183 Browse https://en.wikipedia.org/wiki/Sender_Policy_Framework https://en.wikipedia.org/wiki/DMARC https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

Date	Theme	Goals	Litterature / Preparation
21/5	**Building Robust Networks**	Learn the process of securing a network using security components	Read: ANSM chapter 5,6 - 50 pages, _Campus Network Security: High Level Overview_ NSRC, _Campus Operations Best Current Practice_ NSRC Download, but dont Read:it all https://nsrc.org/workshops/2015/apricot2015/raw-attachment/wiki/Track1Agenda/01-ISP-Network-Design.pdf
23/5	**Running a Modern Network**	Learn that your network is part of the bigger Internet, your security affects others	Browse https://www.manrs.org/ and Read:these https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf https://tools.ietf.org/pdf/bcp38.pdf Skim: RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks
	Summary and prepare for the exam	Summary of the course	Everything read in the primary books, listed above

Introduction and welcome

- Expectations for this course
- Literature list walkthrough
- Kali Linux introduction

Kali Linux is a toolbox we will use and participants will use a virtual machine

Exercises

- Kali Linux installation

TCP/IP and Security in TCP/IP protocol suite

- Addressing and layering OSI model vs internet model
- Network devices Ethernet, bridges, switches, routers
- Common protocols, layer 2 and layer 3
- Secure network design Background paper *Security problems in the TCP/IP protocol suite*, S. M. Bellovin

Exercises

- run tcpdump, wireshark, traceroute, whois

Network Security Threats

- ARP spoofing, ICMP redirects, the classics
- Person in the middle attacks
- Network Scanning
- Intro to routing protocols attacks
- BGP intro and hijacking
- DDoS and flooding

Exercises

- ARP spoofing and ettercap
- EtherApe
- Nmap and Nping
- Pcap-diff https://github.com/isginf/pcap-diff

Traffic inspection and firewalls

- Network sniffing strategies and techniques
- Generic IP Firewalls stateless filtering vs stateful inspection
- Next Generation firewalls, Deep Packet Inspection
- IEEE 802.1q VLAN
- Common countermeasures in firewalls

Exercises

- Nmap scanning basics

Encrypting the network

- Basic cryptography
- Encryption Decryption
- Hashing
- Short introduction to algorithms RSA, AES
- Diffie Helman exchange
- Transport Layer Security (TLS)

Exercise/examples

- mitmproxy https://mitmproxy.org/
- sslsplit https://www.roe.ch/SSLsplit
- sslstrip https://moxie.org/software/sslstrip/
- https://www.ssllabs.com/ and sslscan checking servers

Virtual Private Networks

- IPsec and L2TP/IPsec
- TLS VPN with example OpenVPN
- Linux Wireguard VPN
- Microsoft DirectAccess and VPN (RAS)

Exercises

- go through the ones used by participants, how are they secured why/why not.
- Sniff data without VPN and after VPN turned on

Wifi Security

- Wifi standarder IEEE 802.11
- Authentication Protocols RADIUS, PAP, CHAP, EAP
- Port Based Network Access Control IEEE 802.1x
- Security problems in wireless protocols
- Security problems in wireless encryption
- Hacking wireless networks

Exercise

- Wifi scanning, aka wardriving
- WPA hacking with a short password

Network Management

- SNMP version 2 vs version 3
- Bruteforcing network devices SSH vs SNMP
- Centralized management SSH, Jump hosts
- Monitoring

Exercise

- Run SNMP walk
- Try brute-force SNMP

Network Intrusion Detection

- Intrusion Detection Systems
- NIDS vs HIDS
- Suricata Zeek
- Network Security Data Visualization
- Kibana Dashboards

Exercise

- Run Zeek and Suricata on small pcaps

Network Forensics

- Centralized syslog
- Netflow data
- Collect Network Evidence
- Analyze Network data
- Network Forensics
- Create Incident Reports

Exercises

- Run forensics similar to ENISA examples
- Create a Kibana dashboard for looking at logs

Honeypots

- History of honeypots
- Why use them research, production
- Types of honeypots low vs high interaction
- Honey nets

Exercise

- Run SSH honeypot and try brute-force it

DNS and Email Security

- DNS introduction
- SMTP introduction
- SMTP TLS
- SPF, DKIM, DMARC
- DNSSEC - DNS integrity
- DNS over TLS vs DNS over HTTPS - DNS encryption

Exercises

- Check some examples like how danish banks are using DMARC, and how your own companies can start using it
- SSLscan with SMTP TLS

Building Robust Networks

- Design a robust network
- Isolation and segmentation
- (Routing Security) removed, see Running a Modern Network slide set
- Switch and access security, port security
- (Wireless security) removed - see Wireless Security slide set
- (Using reputation lists) removed - see Network Intrusion Detection slide set

Parts removed, to make room for practical exercises.

Exercise
We will design and build a sample network together

- VLANs, Routing and RPF
- Wifi, WPA and guest network
- Monitoring - setup LibreNMS
- IDS with Zeek and Suricata - if we have time
- Configure port security - if we have time

Running a Modern Network

- BCP38 RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- Mutually Agreed Norms for Routing Security (MANRS) https://www.manrs.org/isps/
- Testing security, evaluating and reporting
- Hardened network device configurations
- Jump hosts and management networks
- DDoS protection
- Check you network from outside RIPEstat, BGPmon

Exercises

- look at your own networks, from the outside