Network Security

Tomas Olovsson

Computer Science and Engineering

Goals with the course

In this course we will:

1. Understand what the problems are
   - **Where** are vulnerabilities present? (TCP, IP, ARP, ...)
   - **How** are networks attacked? (tools and types of bugs)
   - **Learn** from historical mistakes

2. Investigate solutions
   - Security protocols: SSH, SSL/TLS, IPsec, WPA, …
   - Security enhancing devices: firewalls, routers, switches, IDS systems, …

After the course, you will be able to:

- **Perform** penetration tests of systems and products
- **Design** security solutions: choose firewalls, IDS, choose protocols, …
- **Understand** what makes some solutions more secure than other

GU students – Don’t forget…

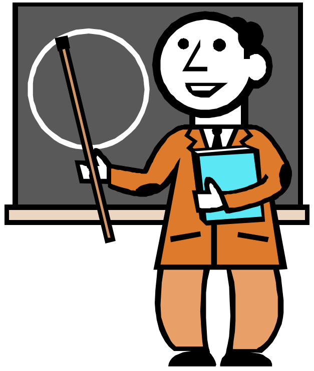
… to register for the course no later than today!

You have to be admitted to the course to participate.

For most courses, there is a waiting list and it is important that we handle the admission of the waiting list in a correct way.

Course information

- Lectures:
  - Tuesdays 13:15 – 15:00
  - Thursdays 13:15 – 15:00
  - Fridays 13:15 – 15:00
  - Not all times will be used, see Canvas pages and Time Edit for details

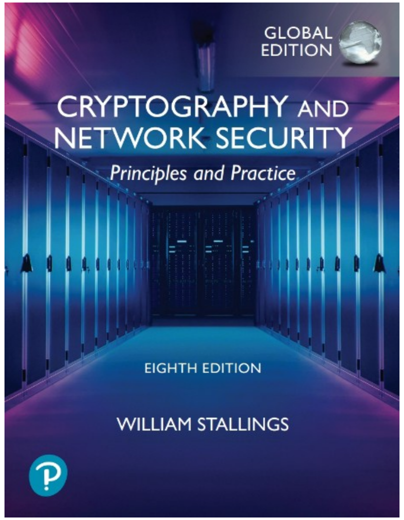


- Lecture hall HC3 – HC2 Thu May 11

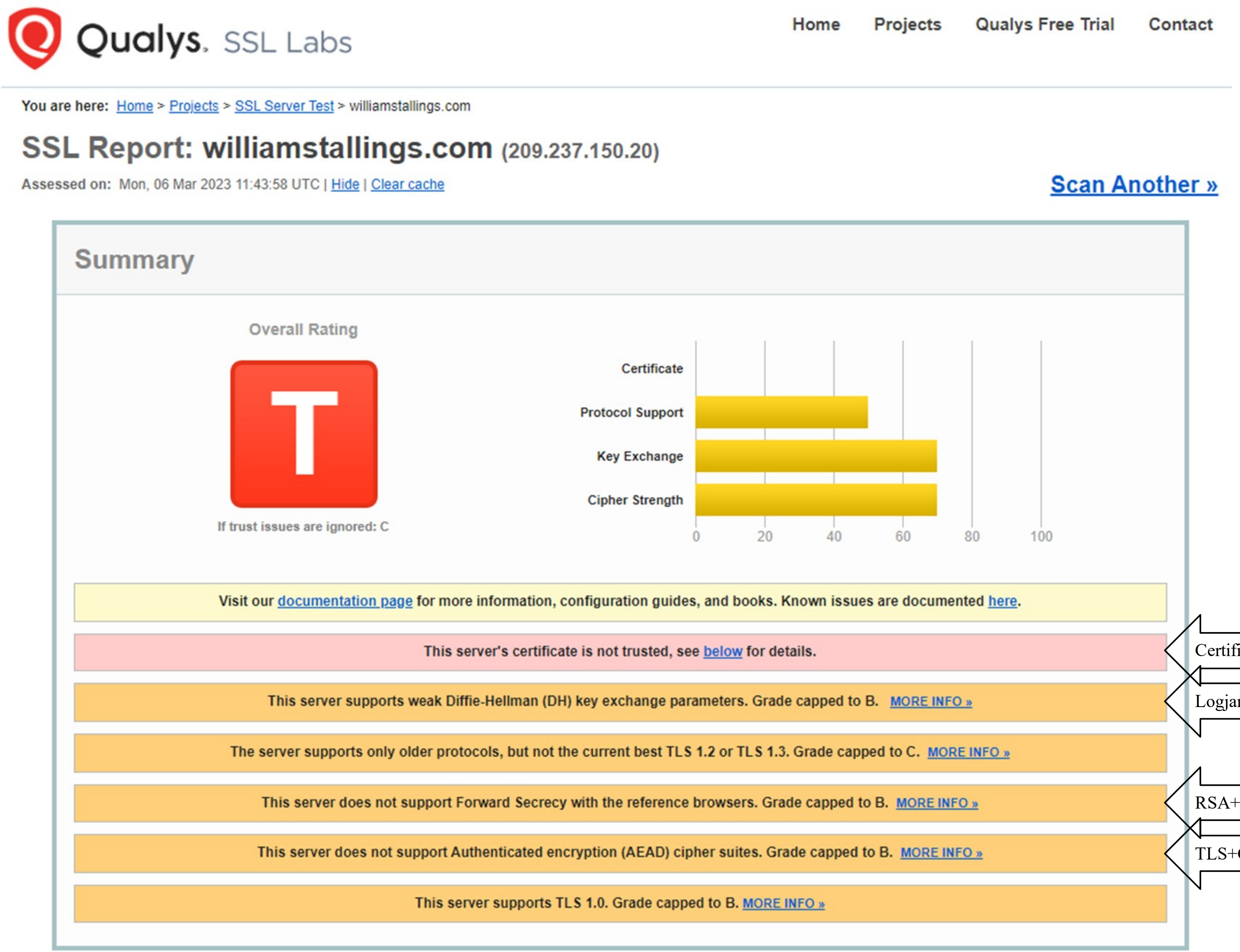
- Course material:
  - **Course book**
  - **Slides** from lectures – preliminary slides can be found on course home page before the lecturers. Download final version after the lecture.
  - **Additional reading** material found on the home page

- Check Canvas regularly for news and info!

The Course Book



- William Stallings: *Cryptography and Network Security,* 8th ed.
  - Shared with the cryptography course
  - 7th edition of the book has on-line web, code for access is in the book
- Companion page created by William Stallings with additional reading material:
  - http://williamstallings.com/Cryptography



You are here: Home > Projects > SSL Server Test > williamstallings.com

SSL Report: williamstallings.com (209.237.150.20)

Assessed on: Mon, 06 Mar 2023 11:43:58 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

T

If trust issues are ignored: C

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2 or TLS 1.3. Grade capped to C. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

This server supports TLS 1.0. Grade capped to B. MORE INFO »

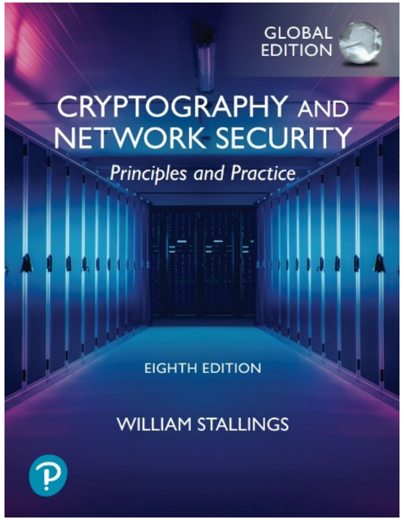
Certificate has expired

Logjam attack

RSA+DH not ok, use ECDHE

TLS+CBC timing attack

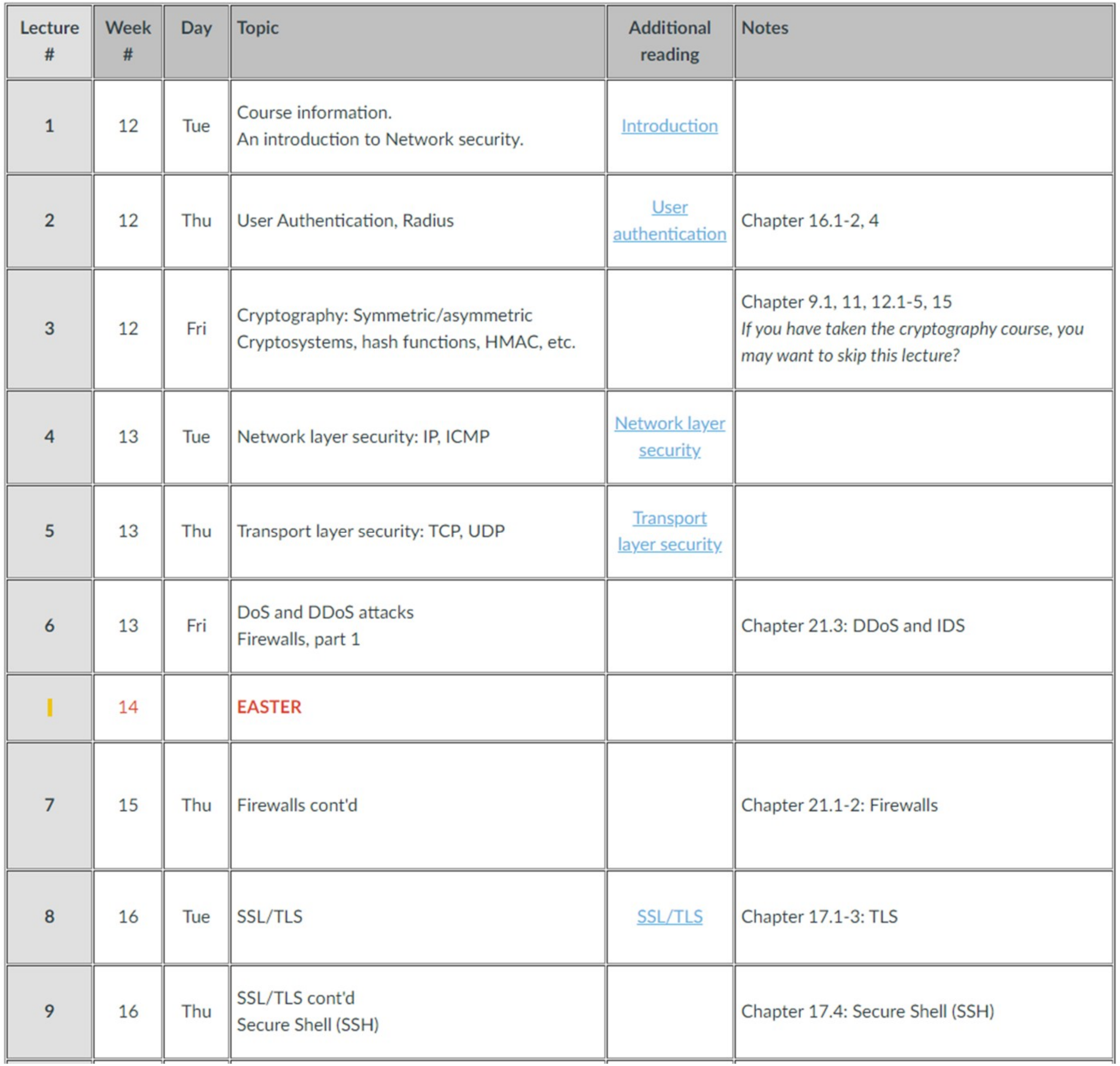
Book chapters



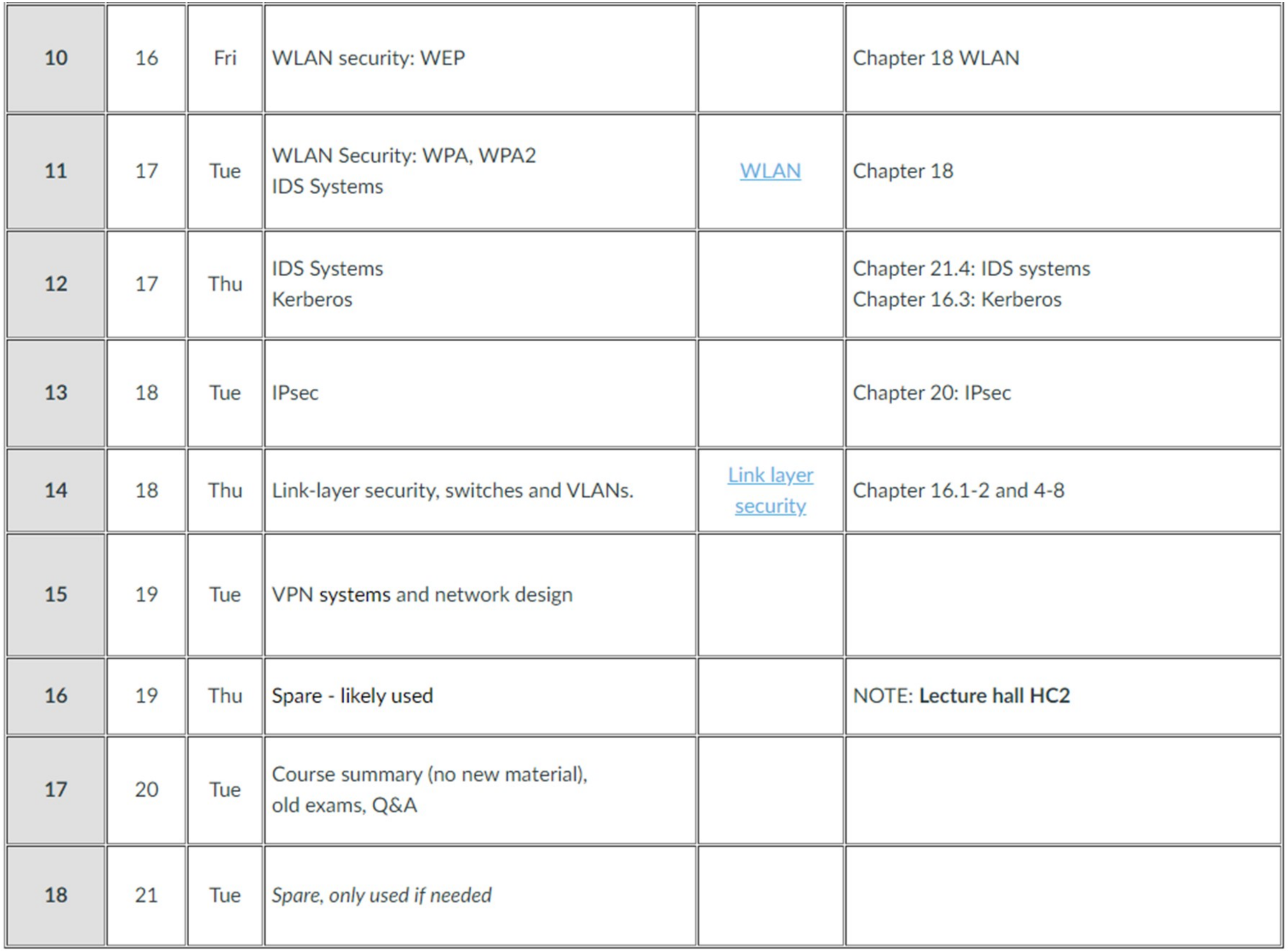
- Chapter 1: Overview, attacks
- Chapter 2 - 14: Cryptography (parts useful also in this course)
- Chapter 15: Key Management and Distribution
- Chapter 16: User Authentication Protocols
- Chapter 17. Transport-Level Security
- Chapter 18. Wireless Network Security
- Chapter 19. Electronic Mail Security
- Chapter 20. IP Security
- Chapter 21. Network Endpoint Security
- Chapter 22. Cloud Security
- Chapter 23. Internet of Things (IoT) Security

Lecture schedule

(preliminary, see Canvas!)



Lecture #	Week #	Day	Topic	Additional reading	Notes
1	12	Tue	Course information. An introduction to Network security.	Introduction	
2	12	Thu	User Authentication, Radius	User authentication	Chapter 16.1-2, 4
3	12	Fri	Cryptography: Symmetric/asymmetric Cryptosystems, hash functions, HMAC, etc.		Chapter 9.1, 11, 12.1-5, 15 *If you have taken the cryptography course, you may want to skip this lecture?*
4	13	Tue	Network layer security: IP, ICMP	Network layer security	
5	13	Thu	Transport layer security: TCP, UDP	Transport layer security	
6	13	Fri	DoS and DDoS attacks Firewalls, part 1		Chapter 21.3: DDoS and IDS
	14		EASTER		
7	15	Thu	Firewalls cont'd		Chapter 21.1-2: Firewalls
8	16	Tue	SSL/TLS	SSL/TLS	Chapter 17.1-3: TLS
9	16	Thu	SSL/TLS cont'd Secure Shell (SSH)		Chapter 17.4: Secure Shell (SSH)



10	16	Fri	WLAN security: WEP		Chapter 18 WLAN
11	17	Tue	WLAN Security: WPA, WPA2 IDS Systems	WLAN	Chapter 18
12	17	Thu	IDS Systems Kerberos		Chapter 21.4: IDS systems Chapter 16.3: Kerberos
13	18	Tue	IPsec		Chapter 20: IPsec
14	18	Thu	Link-layer security, switches and VLANs.	Link layer security	Chapter 16.1-2 and 4-8
15	19	Tue	VPN systems and network design		
16	19	Thu	Spare - likely used		NOTE: **Lecture hall HC2**
17	20	Tue	Course summary (no new material), old exams, Q&A		
18	21	Tue	*Spare, only used if needed*		

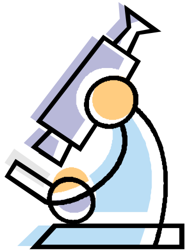
Lab work

- **Lab 1 NMAP:** How to use a scanning tool to scan systems and to use Wireshark to listen to traffic and see system responses.
  All network sniffing must be done in the lab!

- **Lab 2 Firewalls:** To setup and configure a firewall for some services (dns, ftp, web, etc.) and test it using nmap scanning.

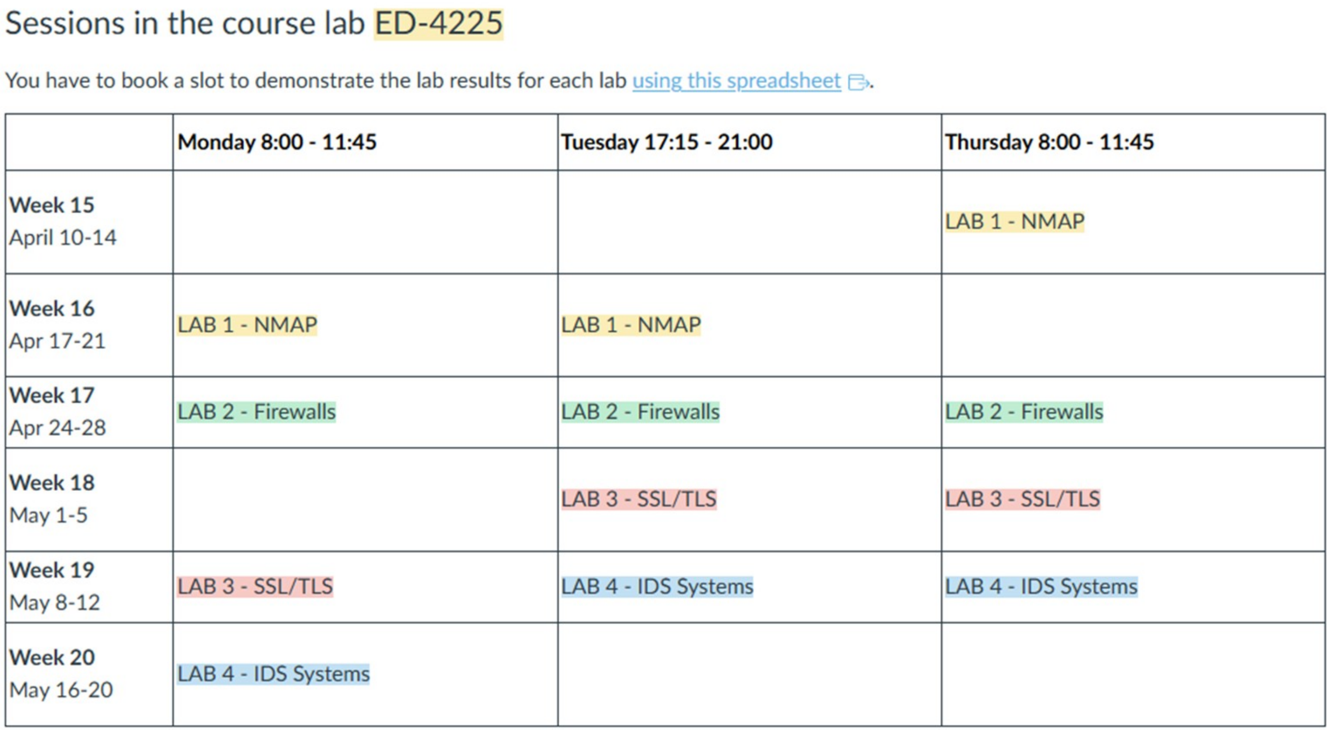
- **Lab 3 TLS:** To work with TLS, generate certificates, understand what level of security it provides.

- **Lab 4 Snort:** Work with an intrusion detection system, to configure the system to send alarms on suspicious network activities.



Lab schedule

Room 4225 (approx. 15 groups at a time)
It’s possible to finish each assignment in one session if you are well prepared ☺



Sessions in the course lab ED-4225

You have to book a slot to demonstrate the lab results for each lab using this spreadsheet.

	Monday 8:00 - 11:45	Tuesday 17:15 - 21:00	Thursday 8:00 - 11:45
Week 15 April 10-14			LAB 1 - NMAP
Week 16 Apr 17-21	LAB 1 - NMAP	LAB 1 - NMAP	
Week 17 Apr 24-28	LAB 2 - Firewalls	LAB 2 - Firewalls	LAB 2 - Firewalls
Week 18 May 1-5		LAB 3 - SSL/TLS	LAB 3 - SSL/TLS
Week 19 May 8-12	LAB 3 - SSL/TLS	LAB 4 - IDS Systems	LAB 4 - IDS Systems
Week 20 May 16-20	LAB 4 - IDS Systems		

The labs should be finished and approved according to this schedule.

You should not work with LAB 1 when LAB 2 has started.

Book only one session each week

Lab work

- Sign up for lab groups in *Canvas group management system*
  - **2 persons** in each group – not more, not less
  - **Lab-related questions should be sent to the teaching assistants (TA:s)**
  - Session bookings will be available in Canvas next week (an announcement will be sent out)
- **If you want to do most of the work outside the lab**, make sure that at least one of you can run the virtual machines (Virtual Box) on your computer!
- The results from each lab must be approved by the TA:s
  - Should be done the week allocated to each lab
  - Special sessions can be booked for “demonstration only”
- Please note that *scanning tools and sniffers may only be used in the VirtualBox network* or on a network which you own - you will be fully responsible for any consequences of scanning third party systems.

Examination

- **Monday May 29 – 08:30-12:30**
  - Re-exam: Thursday Aug 24 – 14:00-18:00
  - Re-exam 2: October
- The examination will be in English
  - Don’t forget to register for the exam
  - You have to answer questions in English
  - No aids are allowed – note that aids were allowed on older exams from 2021
  - Regular exam is *planned* to be digital – re-exams traditional exams on paper
- Older exams are available on the course home page
  - Note that the course changes somewhat each year
  - Answers provided are short versions – you need to write more!
- Advise:
  - Don’t start reading the material too late!
    There are lots of details, it is hard to study the course in a short time…

Course evaluation

- Important for next year’s course that all contribute!
- Feedback about lectures, the book and additional reading material, lab sessions, etc.
- Course representatives 2023:

MPCSN	gaby.arias.b@gmail.com	Maria Arias Buenaño
MPSOF	linde@student.chalmers.se	Filip Linde
MPCSN	martinbjorklund94@gmail.com	Martin Björklund Hultman
MPICT	qinxiaoshu@protonmail.com	Bingcheng Chen
MPCSN	madhuvenkatesh03@gmail.com	Madhumitha Venkatesan

- Info for representatives:
  https://www.chalmers.se/en/education/your-studies/plan-and-conduct-your-studies/course-evaluation/#being-a-student-representative