HALMSTAD UNIVERSITY
Phone +46 35 16 71 00 - www.hh.se
School of Information Technology

Advanced Computer Networks and Security 15 credits

Avancerade datornätverk och säkerhet 15 hp

Second cycle
Main field: Digital Forensics, Second cycle, has only first-cycle course/s as entry requirements (A1N)
Syllabus is adopted by the Research and Education Board (2024-03-20) and is valid for students admitted for the autumn semester 2024.

Placement in the Academic System

The course is included in the Master of Science programme in Network Forensics 60 credits. The course is also offered as a freestanding course.

Prerequisites and Conditions of Admission

Bachelor of Science degree in an engineering subject or in computer science. The degree must be equivalent to a Swedish kandidatexamen and must have been awarded from an internationally recognised university. Courses in computer technology, digital communication, computer networks, computer science or digital forensics of at least 90 higher education credits, of which 15 credits must be in Computer networks and 7.5 credits in Programming. Courses in mathematics of at least 15 higher education credits. English 6. Exemption of the requirement in Swedish is granted.

Course Objectives

The aim of the course is to enable students to develop specialised theoretical and practical knowledge of different computer network protocols, security risks and threats, weaknesses in communication systems and computer networks and the corresponding methods of protection and detection of attacks, and to introduce typical implementations of IoT (the internet of things). A further focus of the course is on the design and practical implementation of security solutions and surveillance in TCP/IP network and the performance of penetration tests of communication systems.

On completion of the course, the students shall be able to

Knowledge and understanding

- describe different protocols of communication systems and computer networks and explain how they work
- classify different types of network attacks and suitable countermeasures
- account for key concepts such as IoT and associated structures.

Skills and ability

- perform advanced configurations of network equipment
- use surveillance tools and systems for detecting trespassing in computer networks and communication systems
- use penetration tests to identify security issues in computer networks and communication systems and propose countermeasures
- present the results of a project in speech and in a written technical report
- plan a systematic security policy taking into account the end user of a computer network and sustainability aspects.

Judgement and approach

- analyse security risks and threats
- reflect on security from a community perspective in terms of network surveillance, personal integrity and social engineering
- take a critical position on current research in the field of network security and digital forensics
- demonstrate awareness of the ethical issues of penetration testing.

Primary Contents

- TCP/IP and OSI models,standards and protocols
- Advanced applied routing andswitching
- Implementations of IoT, for example in health technology and vehicle-to-vehicle communication
- Network security – threats, weaknesses, attacks and countermeasures
- Socialengineering.

- Network surveillance, monitoringand trespassing detection systems
- Penetration testing of communication systems
- Ethical aspects of penetration testing
- Security analysis and sustainable security policies
- Network security from a community perspective
- Report writing
- Presentation techniques.

Teaching Formats

The teaching consists of laboratory exercises, lectures, seminars and a major project which is to be reported in writing and presented orally.

Teaching is in English.

Examination

The overall grades of Fail, 3, 4 or 5 will be awarded for the course.
The assessment is based on laboratory exercises and a practical test, seminars, the oral and written report of the project, and a written exam.

Name of the test		Grading
Laboratory and Practical Tests	4 credits	U/G
Seminars and Oral Presentation	4 credits	U/G
Written Report	3 credits	U/3/4/5
Written Examination	4 credits	U/3/4/5

If there are special reasons, the examiner may make exceptions from the specified examination format and allow a student to be examined in another way. Special reasons can e.g. be a decision on learning support.

For elite sports students according to Riktlinjer för kombinationen studier och elitidrott vid Högskolan i Halmstad, DNR: L 2018/177, the examiner has the right to decide on an adapted examination component or let the student complete the examination in an alternative way.

Course Evaluation

Course evaluation is part of the course. This evaluation should offer guidance in the future development and planning of the course. Course evaluations should be documented and made available to the students.

Course Literature and Other Study Resources

Comer, Douglas E. *Internetworking with TCP/ IP.* Sixth Edition, Addison-Wesley, 2013.

Stallings, W. *Network Security Essentials: Applications and Standards*. 5th Edition, 2018.

Kim, D., Solomon, M. G. *Fundamentals of Information Systems Security.* 3d edition, Jones & Barlett Learning 2018.

Gregg, M. *Certified Ethical Hacker (CEH) Version 9 Study Guid*e, Pearson, 2017.