IMT4741 Intrusion detection and prevention - 2015-2016

Course code:
IMT4741

Course name:
Intrusion detection and prevention

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of the autumn semester

Language of instruction:
English

Expected learning outcomes:
Knowledge

The candidate possesses advanced knowledge in detection and prevention of intrusions in modern computer systems and networks.

The candidate possesses thorough knowledge about theory and scientific methods relevant for intrusion detection.

The candidate is capable of applying his/her knowledge in new fields of intrusion detection and prevention.

Skills

The candidate is capable of analyzing existing theories, methods and interpretations in the field of intrusion detection and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in intrusion detection.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of intrusion detection and prevention.

The candidate is capable of carrying out an independent limited research or development project in intrusion detection under supervision, following the applicable ethical rules.

General competence

The candidate is capable of analyzing relevant professional and research ethical problems in the field of intrusion detection.

The candidate is capable of applying his/her knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with terminology in the field of intrusion detection and prevention.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of intrusion detection and prevention, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

Topic(s):
1. Definition and classification of IDS systems

2. Basic elements of attacks against data networks and their detection

3. Misuse-based IDS

4. Anomaly-based IDS

5. Testing IDS and measuring their performances

Teaching Methods:
Lectures
Laboratory work
Exercises
Project work

Teaching Methods (additional text):
Lectures

Laboratory exercises

Numerical exercises

Project work

The course will be made accessible to both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (ClassFronter).

Form(s) of Assessment:
Written exam, 3 hours
Evaluation of Project(s)

Form(s) of Assessment (additional text):

- Written Exam, 3 hours (counts 70% of the final mark)
- Project evaluation (counts 30% of the final mark)
- Both parts must be passed.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2017/2018.

Re-sit examination:
Re-sit August 2016 for the written examination.

Tillatte hjelpemidler:
D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Examination support:
Calculator, dictionary

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Slobodan Petrovic

Teaching Materials:
Compulsory literature:
None.
Recommended literature:
1. Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000.
2. Jack Koziol, Intrusion Detection with SNORT, SAMS, 2003.
3. David J. Marchette, Computer Intrusion Detection and Network Monitoring - A Statistical Viewpoint, Springer Verlag, 2001.
4. Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.
5. Stephen Northcutt, Judy Novak, Network Intrusion Detection, 3rd edition, New Riders, 2003.

Replacement course for:
IMT5151 Intrusion detection and prevention

Additional information:
In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not and if yes, in which form.

Publish:
Yes