GHENT UNIVERSITY

Course Specifications

Valid in the academic year 2024-2025

Network Security (E008710)

Course size *(nominal values; actual values may depend on programme)*

Credits 6.0 **Study time 180 h**

Course offerings in academic year 2024-2025

A (semester 1)	English	Gent

Lecturers in academic year 2024-2025

Volckaert, Bruno	TW05	lecturer-in-charge

Offered in the following programmes in 2024-2025	crdts	offering
Bridging Programme Master of Science in Bioinformatics(main subject Engineering)	6	A
Master of Science in Bioinformatics(main subject Engineering)	6	A
Master of Science in Computer Science	6	A
Master of Science in Computer Science Engineering	6	A
Master of Science in Computer Science Engineering	6	A
Master of Science in Information Engineering Technology	6	A
Exchange Programme in Computer Science (master's level)	6	A

Teaching languages

English

Keywords

Penetration testing, network reconnaissance, network security, network takeovers, secure virtualization, digital forensics, zero trust systems, incident management, intrusion detection, red team, blue team, purple team

Position of the course

ICT infrastructure is at the heart of both critical and non-critical functionality which as a society we have come to rely upon. With the ongoing digitization (e.g. smart appliances, smart phones, smart homes, smart cities, smart energy grids, cloud-systems) it is essential that the security of this infrastructure is given proper attention.
The goal of this course is to get to know by which methods cyber-attackers will typically attempt to infiltrate or disturb proper functionality of these systems, and – if they gain entry – how they will attempt to gain control over lateral systems and potentially conceal their steps. Armed with this knowledge, setting up proper multi-layered network defences against such attacks will be explained.
This is complementary to courses such as Information Security, which focuses specifically on cryptography and implementations of it at a high level of abstraction; and Software Hacking and Protection, where the behaviour of the system is (either partially or fully) unknown by an attacker, the goal of an attacker is to understand or manipulate the behaviour of this system; and Secure Software Systems, which focuses on (often remotely) exploitable flaws and bugs in software designs and implementations.
This course builds on the knowledge gained in earlier courses on computer architecture, operating systems and computer networking.

Contents

- Network protections (firewalls, DDoS protection services)
- Recon (OSINT, vulnerability / network scanning, web app scanning) to identify and enumerate targets
- Penetration testing (MetaSploit a.o.)
- Remote privilege escalation and client-side attacks
- Lateral network movement

- Intrusion Detection (fingerprinting and heuristics)
- Physical access attacks (drives / devices)
- Social engineering attacks (doppelganger domains, phishing)
- Wireless network takeovers
- Jump-servers, Privileged Access Workstations
- Digital forensics: examining digital devices after a security incident
- Threat modelling (risk factors in network security: where to place key infrastructure / DMZ)
- Secure IoT design - SCALA - other types of networks
- Secure virtualization options: Containers, microVMs, sandboxing, etc.
- Zero trust systems (enclaves, confidential containers, use of rented infrastructure for sensitive payloads, etc.)
- Incident management: practical key / secret management (e.g. in Kubernetes), back-up infrastructure, fault tolerance, administrative access doors

Initial competences

- Programming in C and C++, Python
- Knowledge of computer architecture
- Knowledge of computer networking fundamentals
- Knowledge of operating system internals
- Basic Linux (i.e. Bash) knowledge
- Basic knowledge of databases

Final competences

1 Understand and be able to use the terminology dealing with offensive and defensive network security aspects (red team, blue team, purple team).
2 Deep understanding of reconnaissance techniques (OSINT, vulnerability scanning, etc.).
3 The ability to conduct penetration tests on networked applications and present findings in a professional manner.
4 Likewise the ability to detect unsolicited penetration tests being performed on self-governed infrastructure.
5 Deep understanding of vulnerabilities in networked software, analysis of their impact, and construction of countermeasures to prevent them from being abused.
6 Deep understanding of techniques to secure virtualised orchestrated workloads.
7 Knowledge of zero trust system principles.
8 The ability to design and set up a secured company network which includes public facing services and conversely the ability to penetrate an insecure network.
9 The ability to perform digital forensics on a system that was subject of a security breach.
10 Communicating and presenting domain-specific knowledge in a correct and clear manner, with the appropriate language skills, incl. the use of correct terminology.

Conditions for credit contract

Access to this course unit via a credit contract is determined after successful competences assessment

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Lecture, Practical, Independent work

Extra information on the teaching methods

The students' laptops must be able to run x64 virtual machines.

Study material

Type: Slides

Name: Network Security
Indicative price: Free or paid by faculty
Optional: no
Language : English
Number of Slides : 700
Available on Ufora : Yes
Online Available : Yes
Available in the Library : No
Available through Student Association : No

References

- (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th

Edition, Mike Chapple, James Michael Stewart, Darril Gibson, 2021, ISBN: 978-1-119-78623-8
- CompTIA Security+ Study Guide, 7th Edition, Emmett Dulaney, Chuck Easttom, 2017, ISBN: 978-1-119-41690-6
- The Hacker Playbook: Practical Guide to Penetration Testing (vol 1, 2 and 3), Peter Tim, 2014 (1), ISBN 978-1494932633, 2015 (2), ISBN 978-1512214567, 2018 (3): ISBN 978-1980901754

Course content-related study coaching

- Interactive support and coaching through the electronic learning platform appointments
- Teachers and assistants are available for extra help before and after contact hours, and via e-mail, chat and conf calls

Assessment moments

end-of-term and continuous assessment

Examination methods in case of periodic assessment during the first examination period

Written assessment with open-ended questions

Examination methods in case of periodic assessment during the second examination period

Written assessment with open-ended questions

Examination methods in case of permanent assessment

Participation, Peer and/or self assessment, Assignment

Possibilities of retake in case of permanent assessment

examination during the second examination period is possible in modified form

Extra information on the examination methods

- Periodic evaluation: written examination with open and closed questions on theory, with closed-book
- During semester: graded lab sessions (written reports)

Calculation of the examination mark

- 50% on permanent evaluation, 50% on periodic exam.
- Lack of participation in permanent evaluation for no valid reason results in a zero for that part.
- In the case of group assignments, the students in a group get the same score by default. Only when there is a clear difference in contribution, the students will be given different scores.
- The student must pass (>=10/20) both parts to pass the whole course. If they fail for one part while still scoring >=10/20 on average, the final score becomes 9/20

Facilities for Working Students

Option to be freed from presence in labs after consultation with the responsible teacher (deadline of at least a week for labs). Option for feedback by appointment during and after business hours.