Micro-credential

NETWORK HACKING AND PROTECTION

September – December

GHENT UNIVERSITY

Network Hacking and Protection

CT 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, cloudsystems) 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 multilayered 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.

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

FINAL COMPETENCES

⇨ Understand and be able to use the terminology dealing with offensive and defensive network security aspects (red team, blue team, purple team).
⇨ Deep understanding of reconnaissance techniques (OSINT, vulnerability scanning, etc.).
⇨ The ability to conduct penetration tests on networked applications and present findings in a professional manner.
⇨ Likewise the ability to detect unsolicited penetration tests being performed on self-governed infrastructure.
⇨ Deep understanding of vulnerabilities in networked software, analysis of their impact, and construction of countermeasures to prevent them from being abused.
⇨ Deep understanding of techniques to secure virtualised orchestrated workloads.
⇨ Knowledge of zero trust system principles.
⇨ 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.
⇨ The ability to perform digital forensics on a system that was subject of a security breach.
⇨ Communicating and presenting domain-specific knowledge in a correct and clear manner, with the appropriate language skills, incl. the use of correct terminology.

LECTURER

- **Prof. Bruno Volckaert,** Department of Information Technology, Ghent University

TARGET AUDIENCE

The target audience for this course is ICT-knowledgeable / ICT-curious people with a background in computer science through education or experience. The course explains a variety of stages used by cybercriminals to gain entry into industrial networks, and shows the tools and tricks of the trade that are being used. No new hacks are being developed (so programming skills are seldom used), but one has to be decent with command-line manipulation and scripting, to allow interpreting and employing given tools. The course assumes no prior hacking knowledge.

Participants are expected to:

- Have programming skills in C and C++, Python.
- Have knowledge of computer architecture, of computer networking fundamentals and of operating system internals.
- Have basic Linux (i.e. Bash) knowledge.
- Have basic knowledge of databases.

The language of instruction is English, which requires a sufficient command of the English language.

PRACTICAL INFO

⇨ **FEE** € 393,-
⇨ **LOCATION** Universiteit Gent, Campus Technologiepark Zwijnaarde
⇨ **TIME** September – December

More info? Go to ⇨ **WWW.UGAIN.UGENT.BE/NHP**