Applied Cyber Security

Syllabus Winter Term 2022/23

Prof. Dr. Nils Aschenbruck, Eric Lanfer M. Sc., Till Zimmermann M. Sc.
Document Date: September 1, 2022

Preface

Welcome to the course Applied Cyber Security (ACS) 22/23!

You probably learned several theoretical concepts and methods about cybersecurity in courses offered by our institute. Maybe you even identified a vulnerability on your own in a system or software product. However, in teaching traditional lectures, we sometimes do not have the chance to have a more hands-on view on a certain topic. This year we offer ACS, which will be a very practical 2 week block lab course.

During these two weeks you will get in touch with different formats, we will have some traditional lectures to give you theoretical foundations that will be needed afterwards in the practical sessions. You will also have the chance to learn a security tool by heart and present its functionalities to your fellow students. The core of the course are the Hack the Box sessions, where you get a virtual machine with security issues, and you have to discover and exploit such issues. Instead of writing a traditional report or exam at the end of the course, we will let you work on recent security papers that were presented on high-level security conferences. During the course, you will have some time slots to work on the paper and to create a presentation, which will be presented on the last Friday of the course to your fellow students. With this format, every participant will also gain an insight in recent cybersecurity research.

Introduction

This syllabus will provide you all information on this course, from organizational topics like the schedule, up to references and readings for you at home to intensify your knowledge on some topics. **This is not the final version of the document. It will be published in a few weeks. The current version is only intended to give you a brief overview on what will happen in this course.**

Requirements

Every student participating needs to have passed a course on IT and Network Security (or similar). Since we do not have much time to lay foundations in just two weeks, the knowledge from this course is mandatory.

Course size and selection procedure

Since we are working in the lab for most of the time, we can only offer 20 seats in this course. If more than 20 students enrol, we will prioritize master students, because this course is intended for the master program. In the case of having more than 20 master students enrolled, we will draw lots for the seats. In any case, an IT and network security course passed is necessary.

Course format

The course consists out of six components:

- Lectures (**L**) - Daily lectures will give a basic input for practical topics that will be covered during this course
- Practical sessions (**PS**) - Lab session to learn and work with new tools
- Hack the Box Session (**HTB**) - Lab session where you will get a prepared virtual machine that you have to investigate on
- Preparation Time (**PREP**) - Time for preparation of presentations and reading
- Hands-on Session - Presentation of tools, that were assigned to groups of two
- Paper Presentation Discussion - Presentation of current research papers by the participants

Grading You will be graded based on the presentation each of you will hold at the end of the course. We will provide you a number of papers, where all students have to choose one paper and prepare a presentation on. The presentation should last 10 to 15 minutes. Regular and active participation in the course is required for admission to the final presentation. Without regular and active participation, the practically oriented learning objectives of the course, which are mainly taught in the Lab Sessions, cannot be achieved.

Course organisation

Day	Week 1	Week 2
MON	Introduction, Overview, Organisation	**HTB**: OWASP
	L: Reconnaissance, Enumeration and Scanning I	**HTB**: Review
TUE	**L**: Reconnaissance, Enumeration and Scanning II	**L**: Defense Mechanisms I
	PS: Reconnaissance, Enumeration and Scanning	**PREP**: Presentations
	PREP: Hands-on Session	
WED	**PREP**: Hands-on Session	**L**: Defense Mechanisms II
	Hands-on Session	**PREP**: Presentations
THU	2 x Guest Lecture: Security in Industry	**HTB**: Defense and Blue Team
	L: OWASP Top 10	Presentations
FRI	**HTB**: Introduction, Recon, Scanning	Presentations
	HTB: Review	Closing Session and Social Event

Learning goals

When passing this course, you will:

- Understand reconnaissance, enumeration and scanning methods.
- Be able to apply reconnaissance, enumeration and scanning practically in order to gain information of a system or network.
- Understand basic principles of system security, especially defense mechanisms to protect systems from remote attacks.
- Have an overview on current research topics in the area of cyber security.
- Be able to employ basic security mechanisms on Linux and UNIX based computer system.
- Understand common vulnerabilities in web applications.
- Be able to exploit common vulnerabilities in web applications.
- Be able to use a chain of tools for penetration testing.