Prof. Dr. Alexandra Dmitrienko

https://trust.informatik.uni-due.de/

Module Title

Ethical Hacking Lab

Module Type

Self-paced lecture (online, guided self-learning) with supervised laboratory exercises

Credits

6 ECTS

Language of Instruction

English

Prerequisites

Basic knowledge of computer networks, operating systems, and web technologies is recommended.

Target Group:
This module is designed for Master's-level students in computer science, who seek in-depth knowledge of offensive security techniques and hands-on penetration testing experience.

Module Description

The Ethical Hacking Lab provides students with a comprehensive introduction to offensive security techniques used by ethical hackers and penetration testers. The course combines a theoretical foundation based on an industry-recognized curriculum with an intensive hands-on laboratory phase, enabling students to understand, execute, and critically evaluate common attack techniques in a controlled and ethical environment.

The course emphasizes methodological, legal, and ethical aspects of hacking and penetration testing. Students learn how adversaries think and operate, enabling them to better design, implement, and evaluate effective defensive security measures.

The module consists of two complementary parts:

1. **Theoretical Part**
   Students complete the *Ethical Hacker* course provided by the Cisco Networking Academy (NetAcad). This part introduces core concepts of ethical hacking, penetration testing methodologies, vulnerability assessment, exploitation techniques, post-exploitation activities, and professional reporting.

2. **Practical Laboratory Part**
   In a two-week intensive lab phase, students apply the acquired knowledge in ten supervised hands-on exercises. All activities are conducted in isolated virtual environments under close supervision by university tutors, strictly adhering to ethical and legal guidelines.

Upon successful completion, students receive academic credit for the module and an official Cisco certificate confirming completion of the Ethical Hacker course.

Learning Objectives

After successfully completing this module, students will be able to:

- Explain the principles, scope, and ethical responsibilities of ethical hacking and penetration testing
- Apply structured methodologies for planning and scoping penetration tests
- Identify and exploit vulnerabilities in networks, applications, and systems in controlled environments
- Analyze common attack techniques including network-based, web-based, and protocol-level attacks
- Perform post-exploitation activities and assess their security impact
- Document findings and create professional penetration testing reports
- Use industry-standard tools for offensive security and vulnerability analysis
- Reflect on defensive implications and appropriate mitigation strategies

---

Course Content

Theoretical Part (Cisco Networking Academy – Ethical Hacker)

- Introduction to Ethical Hacking and Penetration Testing
- Planning and Scoping a Penetration Testing Assessment
- Information Gathering and Vulnerability Scanning
- Social Engineering Attacks
- Exploiting Wired and Wireless Networks
- Exploiting Application-Based Vulnerabilities
- Cloud, Mobile, and IoT Security
- Post-Exploitation Techniques
- Reporting and Professional Communication
- Penetration Testing Tools and Code Analysis

Practical Laboratory Part (Supervised Exercises)

The practical part consists of 10 lab sessions, each focusing on a specific attack class:

1. ARP Spoofing and ARP Cache Poisoning
2. DHCP Starvation and Rogue DHCP Servers
3. XML External Entity (XXE) Attacks

4. Cross-Site Scripting (XSS) Attacks – Session Theft and CSRF Evasion
5. Cross-Site Scripting (XSS) Attacks – SOP, CSP, UXSS, and Filters
6. SSL Certification Authorities and Certificate Abuse
7. Insecure TCP Mechanisms (SYN Flooding, Reset, Hijacking)
8. DNS Poisoning and Cache Attacks
9. Denial-of-Service and Command & Control Techniques
10. Tor and Shodan: Anonymity and Internet-Wide Reconnaissance

Each session includes guided setup, attack execution, observation, and structured discussion of security implications and countermeasures.

Teaching and Learning Methods

- Self-paced online learning via Cisco Networking Academy
- Supervised hands-on laboratory sessions
- Guided exercises and tutor feedback
- Group discussions on ethics, legality, and mitigation strategies

---

Assessment / Participation Requirements

Participation in the practical laboratory sessions is **mandatory and requires physical presence**. Attendance is required to successfully complete the module.

Assessment consists of the following:

- Successful completion of the Cisco Ethical Hacker course
- Written multiple choice exam based on Cisco Ethical Hacker materials
- Participation and performance in laboratory exercises
- Successful completion of all exercises

Certification

Students who successfully complete the theoretical part receive an official Cisco Networking Academy Ethical Hacker certificate. Upon fulfilling all module requirements, students receive full academic credit for the course.