YOUR SPECIALISATION AS A CERTIFIED PENETRATION TESTER

The certificate course "Junior Penetration Tester" imparts the craft of detecting and controlled exploitation of security vulnerabilities within a network. Such a penetration test forms the basis for fortifying an IT infrastructure against hacking attacks.

The threat of cyber attacks has gained increasing importance in recent years, both in the business sector and in public institutions and administrations. This is clearly demonstrated by the annual report of the Federal Office for Information Security (BSI). In addition to financially motivated black hat hackers, politically motivated individuals or groups are playing an increasingly significant role. The damages from a single attack can be immense: In 2021, the successful attack on a district triggered Germany's first cyber disaster.

Sooner or later, every network will be targeted by attackers. The key is to be prepared for this scenario and prevent greater damages. A penetration test subjects the entire IT infrastructure of a client to a comprehensive examination of its security. This includes technical aspects as well as organisational, physical, and the human factor. The goal is to identify vulnerabilities, uncover sources of errors, and ultimately enhance security comprehensively.

Graduates of the "Junior Penetration Tester" certificate course receive specialised training in the field of IT security: the practical ability to investigate IT infrastructural vulnerabilities within a company. A certified Junior Penetration Tester can take on supporting activities within a penetration test. This is achieved through practical instruction and the independent application of the learning content.

GOAL & REQUIREMENTS

Goal
The participant masters the standard procedures of a penetration test. They learn about legal foundations, standards, and a selection of different career paths, and can name and categorise them as needed.

They are capable of independently conducting superficial reconnaissance and identifying obvious vulnerabilities. Additionally, the participant is taught the basics of exploiting vulnerabilities to gain a foothold.

The participant is familiar with the differences between exploit frameworks and manual approaches, their advantages and disadvantages, as well as troubleshooting non-functional exploits.

They learn various types of privilege escalation and lateral movement and can apply them under guidance. The participant can appropriately prepare and document discovered vulnerabilities in a target audience-oriented manner.

The course focuses on a high degree of self-directed learning. The participant is consistently introduced to and encouraged in this mindset. They are always urged to independently find solutions to emerging problems, not to give up, and to seek the mentor's help only as a last resort. Furthermore, the participant has the opportunity to give presentations before simulated expert committees and management bodies to strengthen their confident presentation skills.

Requirements
It is recommended to have completed education or studies in the field of computer science and to have experience in the area of system administration. To apply the course contents, knowledge of Linux, understanding of networks, and the use of a system without a graphical interface (using Shell or CMD) are prerequisites.

CONTENT

Participants have access to a specially developed virtual E-LAB during the event and the exam, through which the course contents are taught and tested. The practical implementation of various attack techniques takes centre stage. The course contents are divided into three blocks:

1. **Foundations and Frameworks**
   - Security goals, pillars of IT security
   - Types of hackers
   - Laws and regulations, critical infrastructure (KRITIS)
   - Standards and methods
   - Career paths & IT security professions
   - Relevant certifications, further education opportunities, training labs
   - Project management (Waterfall vs. Agile)
   - Red Teaming vs. Pentesting vs. Vulnerability Analysis
   - CTF vs. Pentesting
   - Phases of an attack/ Kill Chain, Lockheed Martin, PTES, MITRE, etc.

2. **Structure and Process of a Penetration Test**
   - Phases/ Process of a penetration test
   - Objective and results of a penetration test
   - Documentation of vulnerabilities
   - Planning/ Initiation of a penetration test
   - Risks and common mistakes (from practice to practice)
   - Scoping
   - Result presentations for IT & Management

3. **Conducting a Penetration Test**
   - KickOff
   - Information Gathering/ Active /Passive Reconnaissance
   - Fundamentals of countermeasures (FW, IDS, IPS, WAF, EPP, Logging, SIEM) & Security Operations (SOC, CERT, Blue Team, etc.)
   - Vulnerability Analysis and Vulnerability Classification (CVE, CVSS, Exploitability, and Criticality)
   - Dealing with 0-Days Disclosure Types (Responsible, Full)
   - Exploitation/ Low Hanging Fruits (Common Attack Paths like SQL/ Command Injection, Basic Buffer-Overflow, Misconfigurations, etc.)
   - Post Exploitation Basic Privilege Escalation Looting, Persistence, and Lateral Movement/ Low Hanging Fruits
   - Differences On-Premise vs. Cloud
   - Mobile & Web Application Pentesting Basics

CERTIFICATION POLICY

Examination Process

The examination is divided into two sections – the theory part and the practical part. In the theory part, a maximum of 79.5 points is possible, while in the practical part, 90 points are possible. To pass the exam, a total of 110 points is required. The weighting of the two exams is 1:1, making it impossible to pass solely on theoretical knowledge. After submitting the exams, they are corrected, and all participants receive the results on the same day upon passing.

Structure – Theory Part

Multiple-choice questions may have one or more correct answers. Open questions are to be answered with free text. The duration of this part of the exam is 90 minutes. No aids are allowed during the theory exam.

Structure – Practical Part

For the practical exam, participants receive a separate VPN access. Each participant has their own simulated company network. On each system, there are so-called flags, which are obtained by "hacking" individual services, entire systems, or similar. Each flag can be obtained in multiple ways. The scope is communicated before the start of the practical exam. The duration of this part of the exam is 180 minutes. All technical aids are allowed.

GENERAL INFORMATION

Teaching Format:
Full-time in-person at the ProSec GmbH location in Polch or live-online

Completion:
Certificate or Participation Certificate

Duration of Classes:
54 teaching units each lasting 45 minutes

Video Introduction to the Course:
https://youtu.be/VoEt4msIjC0

Our Instructors:
Chris Hein, Head of Detection Services
Christian Horn, Head of Solution Services
Michael Topal, Senior Penetration Tester
Robin Unglaub, Professional Penetration Tester

Who We Are:
https://www.prosec-networks.com/en/ueber-uns/