READY FOR THE NEXT LEVEL?

Graduates of our Junior Penetration Tester (JPT) certificate course have demonstrated their mastery of the fundamental craft of penetration testing at an advanced level. With the Professional Penetration Tester (PPT) certificate, they can prove that they are ready for the next level: independently conducting complex penetration tests, participating in Red Teaming projects, and guiding junior professionals.

GOAL & REQUIREMENTS

Goal
The participant can independently conduct penetration tests. They are capable of performing technical examinations and documenting the results in a target audience-oriented manner. They can conduct comprehensive reconnaissance and identify hidden attack vectors.

They understand the functioning of general security mechanisms in the network and know how to bypass them. Furthermore, they can adapt available exploits to their needs and assess their technical impact on the target system. The participant masters various methods of privilege escalation and understands the basics of covert penetration testing (Red Teaming/OPSEC).

The participant is able to convey technical details to a colleague and middle management in a company. They can propose suitable solutions for identified vulnerabilities. Additionally, they can involve juniors in projects and conduct projects as a team.

Requirements
Successful completion of the JPT is a prerequisite for the PPT, or relevant professional experience as a penetration tester with equivalent manufacturer certifications. 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.

ProSec
Security redefined.

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.

1. **Requirements Analysis**
   - Sizing
   - Service
   - Possible/Relevant Examination Areas

2. **KickOff**
   - Framework Conditions
   - Scoping
   - Communications
   - Status
   - Test Times
   - Scenarios etc.

3. **Execution**
   - Information Gathering (External / Internal - Network / Windows)
   - Functionality & basic bypass methods of countermeasures (Firewalls, Load balancers, VLAN/ACLs, NAC)
   - Vulnerability Analysis (Automated, Manual, Scripted)
   - Exploitation (Controlled exploitation of vulnerabilities, Fuzzing, MITM, Windows Active Directory)
   - Preparation of a Social Engineering scenario
   - Functionality & basic bypass methods of countermeasures (IDS, IPS, WAF, EPP/AV)
   - Post Exploitation (Privilege Escalation, Pivoting, Lateral Movement, OPSEC Basics, Living off the Land)

4. **Conclusion**
   - Documentation
   - Presentation for IT & Management

ProSec
Security redefined.

CERTIFICATION POLICY

Examination Process

The examination is divided into two sections – Theory and Practical. In the Theory section, 79.5 points are possible, and in the Practical section, 90 points are possible. To pass the exam, a total of 110 points is required. The weighting of both 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 270 minutes. All technical aids are allowed.

ProSec
Security redefined.

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:
64 teaching units each lasting 45 minutes

Video Introduction to the Course:
https://www.youtube.com/watch?v=y5kiKLvDA_Y

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

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