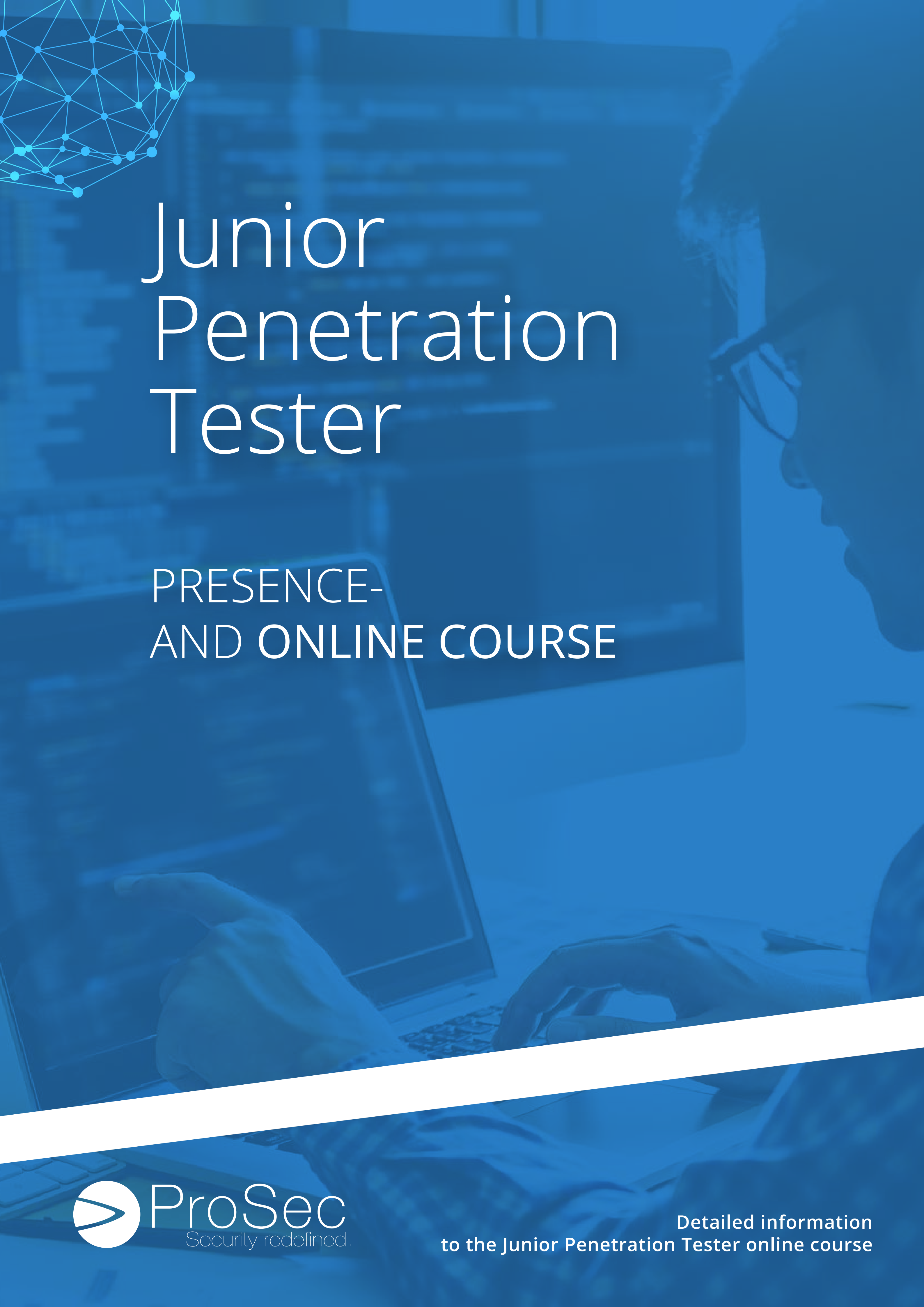

Junior Penetration Tester

PRESENCE- AND ONLINE COURSE

ProSec
Security redefined.

Detailed information to the Junior Penetration Tester online course

Detailed information
to the Junior Penetration Tester Online Course

As an IT security expert with deep knowledge in the field of ethical hacking, ProSec GmbH offers the Junior Penetration Tester (including IHK as a cooperation partner) as a certificate course. This course teaches the craft of detecting security vulnerabilities within a network.

Summary

As a junior penetration tester you have to carry out penetration tests in the team. With the course we enable you to understand penetration test results and interpret them correctly. You can also do small penetration tests after this course.
In the Junior Penetration Tester course we teach you everything you need to know. Building on the legal basis, we move together through a specially prepared hacking lab. The lab does not consist of a flat network, but currently (Since Dec. 2019) contains 151 vulnerable, documented services, separated by security systems in four network areas with different security systems. In the course we will work on all OSI layers together with common attack methods.

Goal setting

Script Kiddies, Kali Linux, Metasploit, Zero day Exploit and Co. are terms that have become more and more established in the media mainstream.
Black hat hackers develop thousands of new exploits every day to exploit vulnerabilities. Many things are already being done to counteract the problem, but cybercriminals are becoming more creative and rigorous. So it´s more important that the IT networks are adequately protected. With so-called penetration tests, computers or networks are subjected to an extensive security check. The aim here is to identify weak points, uncover sources of errors and finally increase security on the technical and organizational level.

As a graduate of the “Junior Penetration Tester” certificate course, a special qualification in the field of IT security is imparted: the practical ability to investigate weak points in the IT infrastructure within a company. With the Junior Penetration Tester, supporting activities can be included in a penetration test.

This is realized through a practice-oriented teaching and the independent application of the learning content. During the course, the participants are in a specially designed E-LAB in which a demilitarized zone (DMZ) is simulated. Participants learn how to hack into a firewalled environment. There are various services in the DMZ that are attacked during the course. In addition to port scans and the various test methods, a cross-section of attack techniques related to OSI layers 1-4 is conveyed. The Junior Penetration Tester offers a well-founded introduction to the technical components for determining weak points. Building on this, we offer the courses for Penetration Tester Web, Penetration Tester Network and Senior Penetration Tester. The advanced certificate seminars are in-depth according to the learning content. In addition, the measures to prevent and close IT infrastructural weak points are taught.

Content

The technology used to convey the content should be emphasized. During the face-to-face event, the participants have access to a virtual E-LAB, which is used to convey the course content, with the focus on the practical implementation of a wide variety of attack techniques.

1. Legal basis

- Framework conditions
- Laws and guidelines
- GDPR (TOM’s)
- Evaluation of one‘s own company

2. Project management

- RACI
- Columbus principle
- Parkinson‘s Law

3. Certifications and careers

- Job market
- Certificates

4. Standards and methods

- What is a penetration test
- PTES
- OSSTMM
- OWASP
- Phases of a hacker attack

5. Structure of the penetration test

- Scoping
- Third-Parties
- Kick-off

6. Intelligence Gathering

- Basics
- Passive
- Active
- Traveling anonymously
- Countermeasures

7. Vulnerability Analysis

- Basics
- Manual Analysis
- Automated Analysis
- Countermeasures

8. Exploitation

- Basics
- Methods
- species
- Frameworks
- Countermeasures

9. Post Exploitation

- Basics
- Enumeration
- Privilege escalation
- Getting stuck in the system (persistence)
- Cover tracks
- Countermeasures

10. Action plans

- Reason
- Construction

11. Presentations

- Technically
- Management

In the first five sections of the course, participants learn the ethical principles of “hacking”. This includes an introduction to the legal situation, guidelines and ethical standards, as well as the standards and the structure of a penetration test. In Sections 6-9, the participants learn the possibilities and the technical structure of a penetration test, starting with the gathering of information to identify the target up to the system and network takeover. In the last two sections, the participant has to prove what he has learned in a realistic lab, in which he takes over systems and documents the vulnerabilities and security gaps found. These practical tasks are very much based on the tasks and activities of an ethical professional hacker.

Course schedule

Evening course

30 Days	30 Lessons Presence 38 Lessons Self study	10 Days, 6–8 Lessons per Week **1. Week** 1x 4 Lessons from 5–8pm **2. Week** 1x 4 Lessons from 5–8pm **3. Week** 2x 4 Lessons each from 5–8pm **4. Week** Exam, 9 a.m. - 2 p.m. (incl. 30 min Break)	180 min practice 90 min theory	High

Weekend-/ Evening course

30 Days	32 Lessons Presence 36 Lessons Self study	6 Days 4–8 Lessons per Week, 2x 6 Lessons Sa. **1. Week** Mi. 4 Lessons from 5–8pm and Sa. 6 Lessons from 9 a.m. - 2 p.m. **2. Week** 4 Lessons from 5–8pm **3. Week** 4 Lessons from 5–8pm each Mo. and Mi. and Sa. 6 UE from 9 a.m. - 2 p.m. **4. Week** Exam incl. Certificate issue	180 min practice 90 min theory	Medium

Online course with Instructor

7 Days, 7 Lessons per Day	52 Lessons Presence 16 Lessons Self study	7 days in a row	180 min practice 90 min theory	Very high

Presence with Instructor

7 Days, 7 Lessons per Day	52 Lessons Presence 16 Lessons Self study	7 days in a row	180 min practice 90 min theory	Very high

Requirement

Completed training or a degree in IT is recommended, but is not required. In order to be able to use the course content, Linux knowledge, network understanding and the use of a system without a graphical user interface (by using from Shell or CMD) are required. IT practical experience as well as understanding is required.

Exam

The exam is divided into 90 minutes of theory and 180 minutes of practice.
The theory test takes place in the ProSec Talovation platform provided specifically for this purpose, usually without aids.
The questions are asked in such a way that either multiple choice answers or free text fields are available.

The practical exam challenges you, we provide you with a simulated network in our hacking lab. In addition to various hacking tools (which you will get nourished in the training), it is about simulating a small penetration test. The task is to obtain flags as a POC for a successful takeover.

Our examiners then evaluate the total number of points based on the points collected in the theoretical part and the flags obtained in the practical part.

You have the option of receiving proof of your qualifications in the form of a certificate. The certificate is not a must, but is very welcome in the CV

Graduation:

If you have successfully completed the certificate examination, you can acquire the “Junior Penetration Tester (IHK)” certificate for a fee. With this certificate you will receive proof that you have acquired the basic knowledge in the field of ethical hacking.

Furthermore, you have the opportunity to specialize in the area of penetration tester and to further expand and use the imparted knowledge. Building on the Junior Penetration Tester certificate course and the specialization, you can then start the Penetration Tester - NW or WEB.

Course planning 2021

Events	Location
01.02.2021 | 8:00 -16:30	Online
01.02.2021 | 8:00 -16:30	Online
01.02.2021 | 8:00 -16:30	Online

We are glad to be here for you - online, by phone and on site

ProSec GmbH
Robert-Koch-Straße 1-9,
D-56751 Polch, Germany
+49 261 45093090
Info@prosec-networks.com