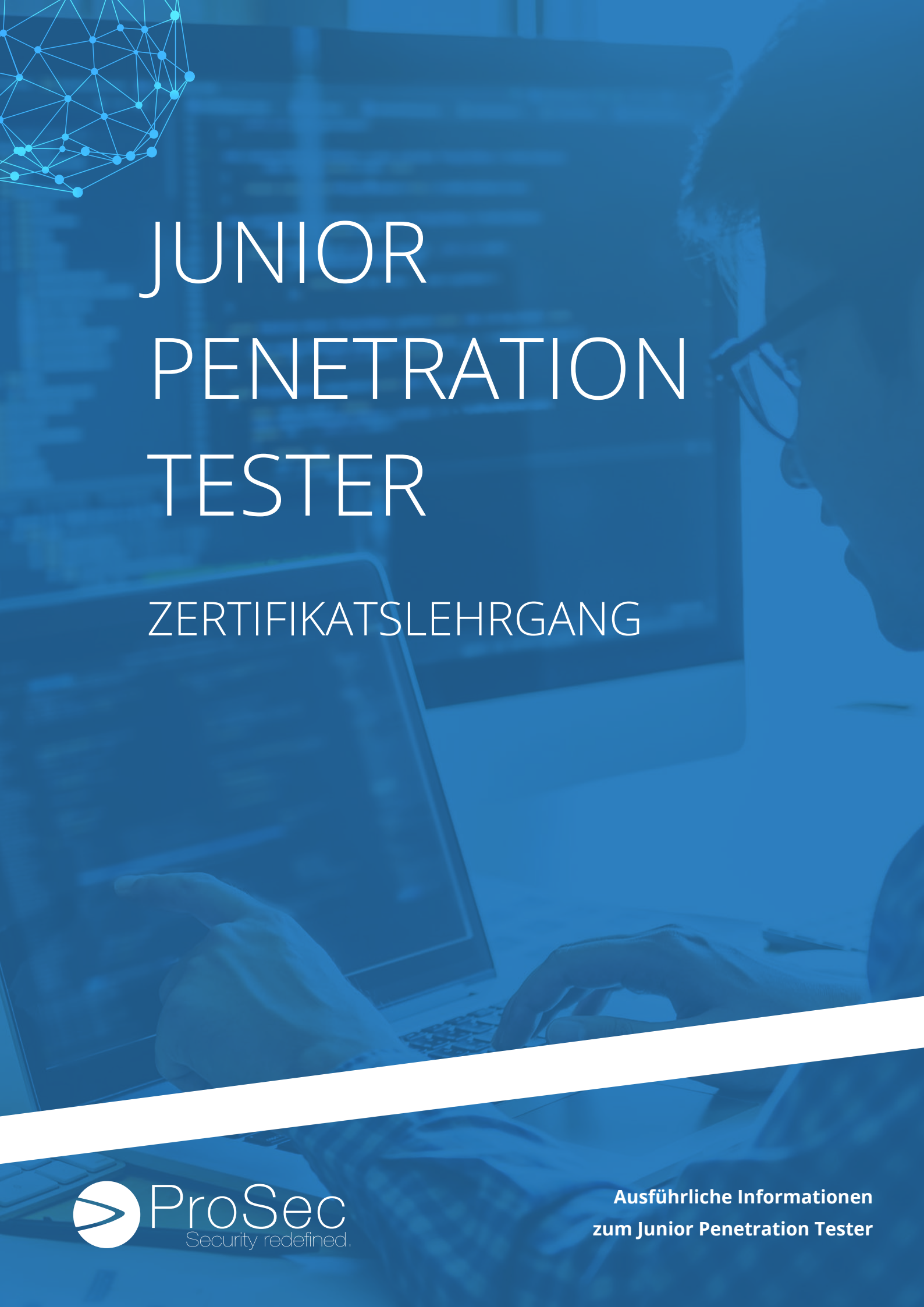

JUNIOR PENETRATION TESTER

ZERTIFIKATSLEHRGANG

ProSec
Security redefined.

Ausführliche Informationen zum Junior Penetration Tester

Dein Einstieg zum zertifizierten Pentester beginnt hier!

Als IT-Sicherheitsexperten mit tiefen Kenntnissen im Bereich des Ethical Hacking bietet die ProSec GmbH den Junior Penetration Tester als Zertifikatslehrgang an. Dieser Kurs vermittelt das Handwerk zur Erkennung von Sicherheitslücken innerhalb eines Netzwerks.

Zusammenfassung

Als Junior Penetration Tester führst du unterstützend im Team Penetration Tests durch. Mit dem Kurs versetzen wir dich in die Lage, die Ergebnisse eines Penetration Tests zu verstehen und richtig interpretieren zu können. Kleine Penetration Tests kannst du nach diesem Kurs ebenfalls durchführen. Im Junior Penetration Tester Kurs vermitteln wir dir alles Notwendige hierzu.

Aufbauend auf den rechtlichen Grundlagen bewegst du dich durch ein speziell präpariertes Hacking Lab. Das Lab besteht nicht aus einem flachen Netzwerk, sondern beinhaltet unterschiedliche angreifbare, dokumentierte Dienste, welche durch Sicherheitssysteme in mehrere Netzwerkbereiche getrennt sind. Neben Portscans und den verschiedenen Prüfmethoden vermittelt der Lehrgang einen Querschnitt an Angriffstechniken, bezogen auf OSI Layer 1-4.

Zielsetzung

Script Kiddies, Kali Linux, Metasploit, Zero day Exploit und Co. sind Begrifflichkeiten, welche sich immer mehr im medialen Mainstream etabliert haben.
Täglich entwickeln „Black Hat Hackers“ Tausende neuer Exploits, um Schwachstellen auszunutzen. Vieles wird schon unternommen, um der Problematik entgegenzuwirken, aber Cyberkriminelle werden immer kreativer und rigoroser. Umso wichtiger ist es, dass IT-Netzwerke ausreichend geschützt sind. Mit sogenannten Penetration Tests werden Rechner oder Netzwerke einer umfangreichen Sicherheits-Prüfung unterzogen. Ziel ist es hierbei, Schwachstellen zu identifizieren, Fehlerquellen aufzudecken und schließlich die Sicherheit auf der technischen und organisatorischen Ebene zu erhöhen.

Als Absolvent des Zertifikatslehrgangs „Junior Penetration Tester“ verfügst du über eine spezielle Qualifizierung im Bereich der IT-Sicherheit: die praktische Befähigung, eine Ermittlung von IT-infrastrukturellen Schwachstellen innerhalb eines

Unternehmens aufzunehmen. Als Junior Penetration Tester kannst du unterstützende Tätigkeiten innerhalb eines Penetration Tests durchführen.

Dies wird durch eine praxisorientierte Vermittlung und dem selbstständigen Anwenden der Lerninhalte realisiert. Während des Lehrgangs und der Prüfung musst du dein gelerntes Wissen in einem realitätsnahen Lab unter Beweis stellen. Dabei musst du Systeme und Dienste enumerieren, Schwachstellen identifizieren, kontrolliert ausnutzen und diese gefundenen Sicherheitslücken dokumentieren.

Neben Portscans und den verschiedenen Prüfmethoden vermittelt der Lehrgang einen Querschnitt an Angriffstechniken, bezogen auf OSI Layer 1-4. Der Junior Penetration Tester bietet einen fundierten Einstieg in die technische Komponente zur Ermittlung von Schwachstellen. Darauf aufbauend bieten wir den Professional Penetration Tester sowie den Senior Penetration Tester an. Diese weiterführenden Zertifikatsseminare sind dem Lerninhalt entsprechend vertiefend. Außerdem werden die Maßnahmen zum Vorbeugen und Schließen von IT-infrastrukturellen Schwachstellen vermittelt.

Inhalte

Hervorzuheben ist die Technik zur Vermittlung der Inhalte. Die Teilnehmer erhalten während der Präsenz-Veranstaltung Zugang zu einem virtuellen E-LAB, mit dem die Kursinhalte vermittelt werden. Dabei steht die praktische Umsetzung der unterschiedlichsten Angriffstechniken im Vordergrund.

THEORIE

1. Projektmanagement

RACI
Columbus Prinzip
Parkinsonsches Gesetz

2. Grundlagen

Schutzziele IT-Sicherheit
Arten von Hackern
Methoden und Motive
Gesetze und Richtlinien
DSGVO (TOM's)
Bewertung des eigenen Unternehmens

3. Standards und Methoden

PTES
OSSTMM
OWASP
Phasen eines Hacker-Angriffs

4. Aufbau Penetrationstest

Scoping
Third-Parties
Kick-off

5. Aktiopnspläne

Nutzen
Aufbau

6. Präsentationen

Technisch
Management

7. Zertifizierung und Karriere

Berufsmarkt
Zertifikate

PRAXIS

1. Information Gathering

Passive
Active

2. Vulnerability Analysis

Manual Analysis
Automated Analysis

3. Exploitation

Frameworks
Password Attacks
Man-in-the-middle
Web Application Attacks
Anonym unterwegs

4. Post Exploitation

Enumeration
Privilege Escalation
Lateral Movement
Sich im System festsetzen (Persistance)
Spuren verwischen

Die Teilnehmer lernen die ethischen Grundlagen des „Hackens“. Dazu gehören die Einführung in die Gesetzeslage, Richtlinien und den ethische Anspruch sowie die Standards und den Aufbau eines Penetrationstests. Des Weiteren lernen die Teilnehmer die Möglichkeiten und den technischen Aufbau eines Penetrations Test beginnend bei der Informationsgewinnung zur Identifizierung des Ziels bis zur System- und Netzwerk-Übernahme.

Während des gesamten Lehrgangs müssen die Teilnehmer ihr gelerntes Wissen in einem realitätsnahen Lab unter Beweis stellen, in dem sie Systeme übernehmen und die gefundenen Schwachstellen und Sicherheitslücken dokumentieren. Diese praktischen Aufgaben orientieren sich sehr stark an den Aufgaben und Tätigkeiten eines ethischen Berufshackers.

Voraussetzung

Wir empfehlen eine abgeschlossene Ausbildung oder ein Studium im IT-Bereich, dieses setzen wir aber nicht voraus. Um die Kursinhalte anwenden zu können, sind Linux Kenntnisse, Netzwerkverständnis sowie die Verwendung eines Systems ohne grafische Oberfläche (durch Nutzung von Shell oder CMD) Voraussetzung. IT-Praxiserfahrung und -Verständnis sind erforderlich.

Prüfung

Die Prüfung ist in 90 Minuten Theorie und 180 Minuten Praxis aufgeteilt.
Die Theorie-Prüfung findet in der eigens dafür zur Verfügung gestellten ProSec Talovation Plattform statt, üblicherweise ohne Hilfsmittel. Die Fragen sind so gestellt, dass entweder Multiple-Choice-Antworten oder Freitext-Felder zur Verfügung stehen.

Für die praktische Prüfung wird ein simuliertes Netzwerk in unserem Hacking-Lab zur Verfügung gestellt.
Neben diversen Hackingtools (welche Bestandteil des Lehrgangs sind) geht es darum, einen kleinen Penetration Test zu simulieren.

Unsere Prüfer werten dann anhand der gesammelten Punkte im theoretischen Teil und den erlangten Flags im praktischen Teil die Gesamtpunktzahl aus.

Abschluss

Bei erfolgreicher Teilnahme an der Zertifikatsprüfung wird das Zertifikat der ProSec GmbH ausgestellt.

Mit diesem Zertifikat wird bestätigt, dass die grundlegenden Kenntnisse im Bereiches des Ethical Hacking vermittelt wurden.

Gegen eine Gebühr kann auch das Zertifikat „Junior Penetration Tester (IHK)" bei der IHK Akademie Koblenz e.V. erworben werden.

Des Weiteren besteht die Möglichkeit, sich auf den Bereich des Penetrationtester zu spezialisieren und die vermittelten Kenntnisse weiter auszubauen und zu nutzen.

Aufbauend auf dem Zertifikatslehrgang „Junior Penetrationtester" und der Spezialisierung kann dann der „Professional Penetration Tester" und darauf aufbauend der „Senior Penetration Tester" erlangt werden.

Dein Ansprechpartner:
Patric Raeschke
Education Services
0261 45093090
p.raeschke@prosec-networks.com

Wir sind gerne für dich da – online, telefonisch und vor Ort

ProSec GmbH
Robert-Koch-Straße 1-9,
D-56751 Polch, Germany
0261 45093090
Info@prosec-networks.com