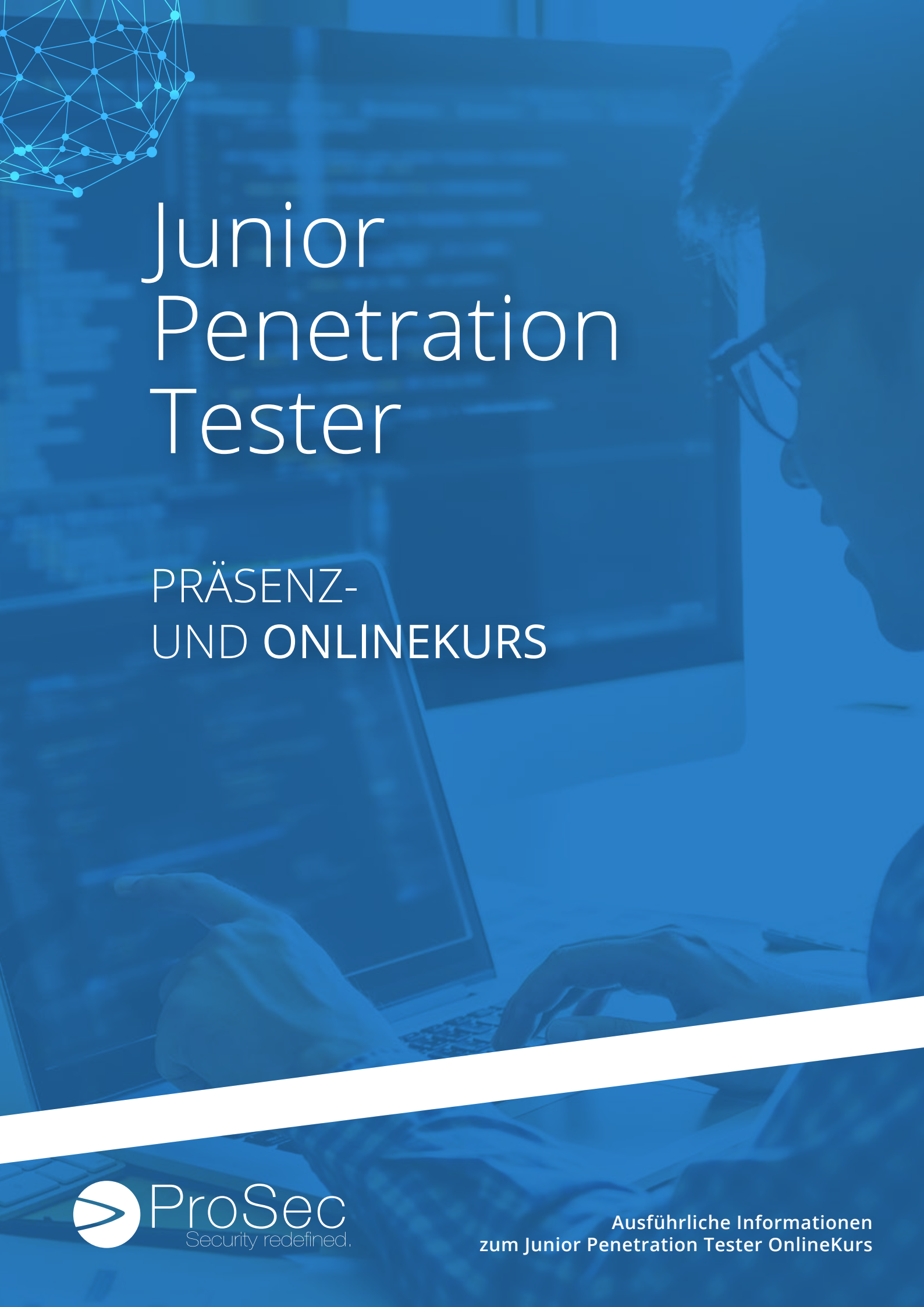

Junior Penetration Tester

PRÄSENZ- UND **ONLINEKURS**

ProSec
Security redefined.

Ausführliche Informationen zum Junior Penetration Tester OnlineKurs

Der Einstieg zum zertifizierten Pentester beginnt hier!

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

Zusammenfassung

Als Junior Penetration Tester musst du unterstützend im Team Penetration Tests durchführen. Mit dem Kurs versetzen wir dich in die Lage, Penetrationstest Ergebnisse 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 bewegen wir uns gemeinsam durch ein speziell präpariertes Hacking Lab. Das Lab besteht nicht aus einem flachen Netzwerk, sondern beinhaltet derzeit (Stand Dez. 2019) 151 angreifbare, dokumentierte Dienste, getrennt durch Sicherheitssysteme in vier Netzwerkbereiche mit unterschiedlichen Sicherheitssystemen. Im Kurs werden wir gemeinsam mit gängigen Angriffsmethoden alle OSI Schichten bearbeiten.

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- Untersuchung 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“ wird eine spezielle Qualifizierung im Bereich der IT-Sicherheit vermittelt: die praktische Befähigung eine Ermittlungen von IT-infrastrukturellen Schwachstellen innerhalb eines Unternehmens aufzunehmen. Beim Junior Penetration Tester können unterstützende Tätigkeiten innerhalb eines Penetration-Tests aufgenommen werden.

Dies wird durch eine praxisorientierte Vermittlung und dem selbstständigen Anwenden der Lerninhalte realisiert. Während des Lehrgangs befinden sich die Teilnehmer in einem eigens konzipierten E-LAB, in der eine demilitarisierte Zone (DMZ) simuliert wird. Die Teilnehmer erlernen, die durch eine Firewall abgetrennte Umgebung zu hacken. In der DMZ befinden sich verschiedene Services, die während des Kurses angegriffen werden. Neben Portscans und den verschiedenen Prüfmethoden wird ein Querschnitt an Angriffstechniken, bezogen auf OSI Layer 1-4, vermittelt. Der Junior Penetration Tester bietet einen fundierten Einstieg in die technische Komponente zur Ermittlung von Schwachstellen. Darauf aufbauend bieten wir den Penetration Tester Web, den Penetration Tester Network sowie den Senior Penetration Tester an. Die 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 Präsenzveranstaltung Zugang zu einem virtuellen E-LAB, mit dem die Kursinhalte vermittelt werden, wobei die praktische Umsetzung der unterschiedlichsten Angriffstechniken im Vordergrund steht.

1. Rechtliche Grundlagen

- Rahmenbedingunen
- Gesetze und Richtlinien
- DSGVO (TOM's)
- Bewertung des eigenen Unternehmens

2. Projektmanagement

- RACI
- Columbus Prinzip
- Parkinsonsche Gesetz

3. Zertifizierungen und Karriere

- Berufsmarkt
- Zertifikate

4. Standards und Methoden

- Was ist ein Penetrationstest
- PTES
- OSSTMM
- OWASP
- Phasen eines Hackerangriffs

5. Aufbau Penetrationstest

- Scoping
- Third-Parties
- Kick-off

6. Intelligence Gathering

- Grundlagen
- Passive
- Active
- Anonym unterwegs
- Gegenmaßnahmen

7. Vulnerability Analysis

- Grundlagen
- Manual Analysis
- Automated Analysis
- Gegenmaßnahmen

8. Exploitation

- Grundlagen
- Methoden
- Arten
- Frameworks
- Gegenmaßnahmen

9. Post Exploitation

- Grundlagen
- Enumeration
- Privelege Escalation
- Sich im System festsetzen (Persistance)
- Spuren verwischen
- Gegenmaßnahmen

10. Aktionspläne

- Begründung
- Aufbau

11. Präsentationen

- Technisch
- Management

In den ersten fünf Abschnitten des Lehrgangs lernen die Teilnehmer die ethischen Grundlagen des „Hackens“. Dazu gehört die Einführung in die Gesetzeslage, Richtlinien und der ethische Anspruch, sowie wie die Standards und den Aufbau eines Penetrationstests. In den Abschnitten 6-9 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. In den letzten beiden Abschnitten muss der Teilnehmer sein gelerntes Wissen in einem realitätsnahen Lab unter Beweis stellen, in dem er Systeme übernimmt und die gefundenen Schwachstellen und Sicherheitslücken dokumentieren. Diese praktischen Aufgaben orientieren sich sehr stark an den Aufgaben und Tätigkeiten eine ethischen Berufshackers.

Kursvariatonen

Abendkurs

30 Tage	30 UE* Präsenz 38 UE* Selbststudium	10 Tage, 6–8 UE* pro Woche **1. Woche** 1x 4 UE* von 17–20 Uhr **2. Woche** 1x 4 UE* von 17–20 Uhr **3. Woche** 2x 4 UE* jeweils von 17–20 Uhr **4. Woche** Prüfung, 9–14 Uhr (inkl. 30 min Pause)	180 min Praxis 90 min Theorie	Hoch

Wochened-/ Abendkurs

30 Tage	32 UE* Präsenz 36 UE* Selbststudium	6 Tage 4–8 UE* pro Woche, 2x 6 UE* Sa. **1. Woche** Mi. 4 UE* von 17–20 Uhr und Sa. 6 UE* von 9-14 Uhr **2. Woche** 4 UE* von 17–20 Uhr **3. Woche** 4 UE* von 17–20 Uhr jeweils am Mo. und am Mi. und Sa. 6 UE von 9-14 Uhr **4. Woche** Prüfung inkl. Zertifikatsausgabe	180 min Praxis 90 min Theorie	Mittel

Onlinekurs mit Dozent

7 Tage, 7 UE* pro Tag	52 UE* Präsenz 16 UE* Selbststudium	7 Tage am Stück	180 min Praxis 90 min Theorie	Sehr Hoch

Präsenz mit Dozent

7 Tage, 7 UE* pro Tag	52 UE* Präsenz 16 UE* Selbststudium	7 Tage am Stück	180 min Praxis 90 min Theorie	Sehr Hoch

Voraussetzung

Es empfiehlt sich eine abgeschlossene Ausbildung oder Studium im IT-Bereich, wird aber nicht vorausgesetzt. 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, sowie Verständnis ist 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, das entweder Multiplechoice Antworten oder Freitext-Felder zur Verfügung stehen.

Die praktische Prüfung geht ins eingemachte, wir stellen Ihnen dafür ein simuliertes Netzwerk in unserem Hacking-Lab zur Verfügung.
Neben diversen Hackingtools(denen Sie in der Schulung nährgebracht bekommen) geht es darum einen kleinen Penetration Test zu simulieren. Die Aufgabe besteht darin Flags als POC zur erfolgreichen Übernahme zu erlangen.

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

Sie haben die Möglichkeit einen Nachweis über Ihre erlangten Qualifikation in Form eines Zertifikats zu erhalten. Das Zertifikat ist kein Muss, wird aber in der CV sehr gerne gesehen

Abschluss:

Bei erfolgreicher Teilnahme an der Zertifikatsprüfung können Sie gegen eine Gebühr das Zertifikat „Junior Penetration Tester (IHK)" erwerben. Mit diesem Zertifikat erhalten Sie den Nachweis, dass Ihnen die grundlegenden Kenntnisse im Bereiches Ethical Hacking vermittelt wurden.

Des Weiteren haben Sie die Möglichkeit sich auf den Bereich des Penetrationtester zu spezialisieren und die vermittelnden Kenntnisse weiter auszubauen und zu nutzen. Aufbauend auf dem Zertifikatslehrgang Junior Penetrationtester und der Spezialisierung können Sie dann den Penetration Tester – NW oder WEB starten.

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

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