PECB BEYOND RECOGNITION

PECB Certified
Lead Ethical Hacker

Erweitern Sie Ihr Wissen über ethisches Hacking und IT-Sicherheit, verbessern Sie Ihre Hacking-Fähigkeiten und perfektionieren Sie Ihr Wissen über die fortschrittlichsten Techniken der IT-Sicherheit.

Warum sollten Sie teilnehmen?

Da die Auswirkungen von Sicherheitsvorfällen in kleinen und großen Organisationen deutlich zugenommen haben, ist auch die Nachfrage nach Ethical Hacking gestiegen. Ethical Hacking ist eines der effektivsten Werkzeuge zur Sicherung von Vermögenswerten und zum Schutz von Menschen und Informationen. Die Ethical-Hacking-Zertifizierung wird langsam zu einer Standardanforderung für Fachleute, die im Bereich der Informationssicherheit arbeiten wollen.

Mit einer PECB Certified Lead Ethical Hacker-Zertifizierung weisen Sie Ihre Fähigkeit nach, die Sicherheit von Systemen rechtmäßig zu bewerten und deren Schwachstellen zu entdecken. Die Schulung vermittelt Informationen über die neuesten Methoden und Werkzeuge des Ethical Hacking. Außerdem wird eine Methodik zur Durchführung von Durchdringungstests in Übereinstimmung mit Standards und Best Practices vermittelt, wie dem Penetration Testing Execution Standard (PTES) und der Open Source Security Testing Methodology (OSSTMM).

Das Verstehen der Strategien von Hackern hilft bei der Lösung von Sicherheitsproblemen und Herausforderungen. Nach dem Besuch des Trainings sind Sie in der Lage, Durchdringungstests zur Informationssicherheit zu planen, zu verwalten und durchzuführen.

Die PECB Certified Lead Ethical Hacker-Training basiert auf dem Konzept, das Gelernte zu üben. Es beinhaltet Labor-Sitzungen und praktische Beispiele, um Ihnen zu helfen, die Theorie in die Praxis umzusetzen.

Im Anschluss an das Training findet eine Prüfung statt. Wenn Sie die Prüfung bestehen, können Sie sich für den Titel "PECB Certified Lead Ethical Hacker" bewerben. Weitere Informationen über den Prüfungsprozess finden Sie im Abschnitt Prüfung, Zertifizierung und allgemeine Informationen weiter unten.

Wer sollte teilnehmen?

Dieses Trainings ist gedacht für:

- Personen, die Kenntnisse über die wichtigsten Techniken zur Durchführung von Durchdringungstests erwerben möchten
- Personen, die in der Informationssicherheit tätig sind und Techniken des Ethical Hacking und Durchdringungstests beherrschen möchten
- Personen, die für die Sicherheit von Informationssystemen verantwortlich sind, wie z. B. Informationssicherheitsbeauftragte und Cybersicherheitsexperten
- Mitglieder von Informationssicherheitsteams, die ihr Wissen über Informationssicherheit erweitern möchten
- Manager oder Fachberater, die lernen möchten, wie man ethische Hacking-Aktivitäten steuert
- Technische Experten, die lernen möchten, wie man einen Penetrationstest plant und durchführt

Kursagend

Dauer: 5 Tag

Tag 1 | Einführung in Ethical Hacking

- Ziele und Aufbau des Trainingskurses
- Durchdringungstest-Standards, -Methoden und -Frameworks
- Überblick über das Labor
- Grundlegende Konzepte des Ethical Hacking
- Netzwerk-Grundlagen
- Verständnis der Kryptographie
- Relevante Trends und Technologien
- Kali Linux-Grundlagen
- Initiierung des Durchdringungstests
- Analyse des Umfangs des Durchdringungstests
- Rechtliche Implikationen und vertragliche Vereinbarung

Tag 2 | Initiierung der Aufklärungsphase

- Passive reconnaissance
- Active reconnaissance
- Identifikation von Sicherheitslücken

Tag 3 | Einleiten der Exploitation-Phase

- Bedrohungsmodell und Angriffsplan
- Umgehen von Intrusion Detection Systemen
- Server-seitige Angriffe
- Client-seitige Angriffe
- Angriffe auf Web-Anwendungen
- WIFI-Angriffe
- Privilegienerweiterung
- Pivotierung
- Dateiübertragungen
- Aufrechterhaltung des Zugriffs

Tag 4 | Post-Exploitation und Berichterstattung

- Aufräumen und Zerstören von Artefakten
- Erzeugen eines Befundberichts
- Empfehlungen zur Abschwächung der identifizierten Schwachstellen
- Abschluss des Trainingskurses

Tag 5 | Zertifizierungsprüfung

Lernziele

Dieses Training ermöglicht es Ihnen,:

- Beherrschen der Konzepte, Methoden und Techniken, die von Cybersecurity-Organisationen und ethischen Hackern zur Durchführung von Durchdringungstests verwendet werden
- Erkennen Sie den Zusammenhang zwischen Penetrationstest-Methoden, gesetzlichen Rahmenbedingungen und Standards
- Erwerben Sie ein umfassendes Wissen über die Komponenten und Abläufe des Ethical Hacking

Prüfung

Dauer: 6 Stunde

Die Prüfung "PECB Certified Lead Ethical Hacker" erfüllt alle Anforderungen des PECB Examination and Certification Program (ECP). Sie deckt die folgenden Kompetenzbereiche ab:

Bereich 1 | Werkzeuge und Techniken zur Informationsbeschaffung

Bereich 2 | Bedrohungsmodellierung und Schwachstellenerkennung

Bereich 3 | Ausbeutungstechniken

Bereich 4 | Privilegieneskalation

Bereich 5 | Pivotierung und Dateitransfer

Bereich 6 | Reporting

Die Prüfung zum PECB Certified Lead Ethical Hacker besteht aus zwei Teilen: der praktischen Prüfung und dem Verfassen eines Berichts. Bei der praktischen Prüfung muss der Kandidat mindestens zwei Zielrechner durch Durchdringungstests kompromittieren. Der Vorgang sollte in einem schriftlichen Bericht dokumentiert werden. Die Prüfung zum PECB Certified Lead Ethical Hacker ist eine Open-Book-Prüfung. Die Kandidaten dürfen während des Prüfungsprozesses Schulungsunterlagen und persönliche Notizen verwenden.

Spezifische Informationen über die Art der Prüfung, die verfügbaren Sprachen und andere Details finden Sie in der Liste der PECB-Prüfungen und Prüfungsregeln und -richtlinien.

Zertifizierung

Nach erfolgreichem Abschluss der Prüfung können Sie sich je nach Erfahrungsstand für das Zertifikat "PECB Certified Lead Ethical Hacker" bewerben, wie in der Tabelle unten dargestellt. Sie erhalten das Zertifikat, wenn Sie alle relevanten Bildungs- und Berufsanforderungen erfüllen.

Weitere Informationen zu Ethical-Hacking-Zertifizierungen und dem PECB- Zertifizierungsprozess finden Sie in den Zertifizierungsregeln und -richtliniene.

Berechtigungsnachweis	Exam	Professional experience	Project experience	Other requirements
PECB Zertifizierter Lead Ethical Hacker	PECB-Prüfung zum Certified Lead Ethical Hacker	2 Jahre Erfahrung im Bereich Durchdringungstests und Cybersicherheit	Keine	Unterzeichnung des PECB- Verhaltenskodex und des PECB- CLEH-Verhaltenskodex

Allgemeine Informationen

- Die Teilnehmer erhalten Trainingsmaterialien mit über 450 Seiten Informationen, Praxisbeispielen und Übungen.
- Eine Bescheinigung über den Abschluss des Kurses im Wert von 35 CPD-Leistungspunkten(Continuing Professional Development) wird für die Teilnehmer ausgestellt, die den Kurs besucht haben.
- Kandidaten, die den Schulungskurs absolviert haben, aber die Prüfung nicht bestanden haben, sind berechtigt, diese einmal innerhalb von 12 Monaten ab dem ursprünglichen Prüfungsdatum kostenlos zu wiederholen.