DEINE SPEZIALISIERUNG ZUM ZERTIFIZIERTEN PENETRATION TESTER

Der Zertifikatslehrgang „Junior Penetration Tester“ vermittelt das Handwerk zur Erkennung und kontrollierten Ausnutzung von Sicherheitslücken innerhalb eines Netzwerks. Ein solcher Penetration Test bildet die Basis für die Härtung einer IT Infrastruktur gegen Hacking Angriffe.

Die Bedrohung durch Cyber Attacken hat in den vergangenen Jahren zunehmend an Bedeutung gewonnen – in der Wirtschaft ebenso wie in öffentlichen Einrichtungen und Verwaltungen. Das zeigt der jährliche Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) sehr deutlich. Neben finanziell motivierten Black Hat Hackern spielen politisch motivierte Einzeltäter oder Gruppierungen eine immer größere Rolle. Die Schäden durch einen einzelnen Angriff sind teilweise immens: Im Jahr 2021 löste die erfolgreiche Attacke auf einen Landkreis den erste Cyber-Katastrophenfall Deutschlands aus.

Früher oder später wird jedes Netzwerk in das Visier von Angreifern geraten. Entscheidend ist, auf diesen Fall vorbereitet zu sein und so größere Schäden zu verhindern. Ein Penetration Tests unterzieht die gesamte IT Infrastruktur eines Kunden einer umfangreichen Untersuchung auf ihre Sicherheit. Dies bezieht technische Aspekte ebenso ein wie organisatorische und physische sowie den Faktor Mensch. Ziel ist es hierbei, Schwachstellen zu identifizieren, Fehlerquellen aufzudecken und schließlich die Sicherheit ganzheitlich zu erhöhen.

Den Absolventen des Zertifikatslehrgangs „Junior Penetration Tester“ wird eine spezielle Qualifizierung im Bereich der IT-Sicherheit vermittelt: die praktische Befähigung, Ermittlungen von IT-infrastrukturellen Schwachstellen innerhalb eines Unternehmens aufzunehmen. Ein zertifizierter Junior Penetration Tester kann unterstützende Tätigkeiten innerhalb eines Penetration Tests übernehmen. Dies wird durch eine praxisorientierte Vermittlung und das selbstständige Anwenden der Lerninhalte realisiert.

ZIEL & VORAUSSETZUNGEN

Ziel
Der Teilnehmer beherrscht das standardmäßige Vorgehen eines Penetration Tests. Er lernt gesetzliche Grundlagen und Standards sowie eine Auswahl unterschiedlicher Karrierepfade kennen und kann diese bei Bedarf nennen und kategorisieren.

Er ist in der Lage, eigenständig oberflächliche Reconnaissance durchzuführen, und offensichtliche Schwachstellen zu erkennen. Weiterhin werden dem Teilnehmer die Grundlagen der Ausnutzung von Schwachstellen zum Erlangen eines Footholds vermittelt.

Unterschiede von Exploit-Frameworks zu manuellem Vorgehen, deren Vor- und Nachteile sowie das Troubleshooting nicht funktionsfähiger Exploits sind dem Teilnehmer bekannt.

Der Teilnehmer lernt unterschiedliche Arten der Privilege Escalation und des Lateral Movement kennen und kann diese unter Anleitung anwenden. Er kann gefundene Schwachstellen angemessen und zielgruppengerecht aufbereiten und dokumentieren.

Im Fokus des Kurses liegt die hohe Ausprägung des autodidaktischen Lernens. Der Teilnehmer wird kontinuierlich an diese Denkweise herangeführt und bestärkt. Er wird stets ermutigt, eigenständig Lösungen für auftretende Probleme zu finden, nicht aufzugeben und erst als letztes verfügbares Mittel den Mentor um Hilfe zu bitten. Des Weiteren wird dem Teilnehmer die Möglichkeit geboten, Präsentationen vor simulierten Fachgremien und Management-Instanzen zu halten, um das selbstbewusste Auftreten zu stärken.

Voraussetzungen
Es empfiehlt sich eine abgeschlossene Ausbildung oder Studium im Bereich der Informatik und Erfahrung im Gebiet der Systemadministration. 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.

INHALT

Die Teilnehmer erhalten während der Veranstaltung und der Prüfung Zugang zu einem eigens hierfür entwickelten virtuellen E-LAB, mit dem die Kursinhalte vermittelt und geprüft werden. Dabei steht die praktische Umsetzung der unterschiedlichsten Angriffstechniken im Vordergrund. Die Kursinhalte sind in drei Blöcke unterteilt:

1. **Grundlagen und Rahmenbedingungen**
    - Schutzziele, Säulen der IT-Sicherheit
    - Arten von Hackern
    - Gesetze und Richtlinien, KRITIS
    - Standards und Methoden
    - Karrierepfade & IT-Security-Berufe
    - Einschlägige Zertifizierungen, Weiterbildungsmöglichkeiten, Trainingslabs
    - Projektmanagement (Wasserfall vs. Agile)
    - Red Teaming vs. Pentesting vs. Schwachstellenanalyse
    - CTF vs. Pentesting
    - Phasen eines Angriffes/ Kill Chain, Lockheed Martin, PTES, MITRE etc.

2. **Aufbau und Ablauf eines Penetration Tests**
    - Phasen/ Ablauf eines Penetration Tests
    - Ziel und Ergebnis eines Penetration Tests
    - Dokumentation von Schwachstellen
    - Planung/ Initiierung eines Penetration Tests)
    - Risiken und common mistakes (aus der Praxis für die Praxis)
    - Scoping
    - Ergebnispräsentationen für IT & Management

3. **Durchführung eines Penetration Tests**
    - KickOff
    - Information Gathering/ Active /Passive Reconnaissance
    - Grundlagen Gegenmaßnahmen (FW, IDS, IPS, WAF, EPP, Logging, SIEM) & Security Operations (SOC, CERT, Blue Team etc.)
    - Vulnerability Analysis und Schwachstellen Klassifizierung (CVE, CVSS, Ausnutzbarkeit und Kritikalität)
    - Umgang mit 0-Day's Disclosure Arten (Responsible, Full)
    - Exploitation/ Low Hanging Fruits (Common Attack Paths wie SQL/ Command Injection, Basic Buffer-Overflow, Misconfigurations, etc.)
    - Post Exploitation Basic Privilege Escalation Looting, Persistence and Lateral-Movement/ Low Hanging Fruits

ZERTIFIZIERUNGSRICHTLINIE

Prüfungsablauf
Die Prüfung untergliedert sich in zwei Abschnitte – Theorie- und Praxisteil.
Im Theorieteil sind 79,5 Punkte möglich. Im Praxisteil sind 90 Punkte möglich. Zum Bestehen der Prüfung sind 110 Punkte notwendig. Die Gewichtung der beiden Prüfungen erfolgt hierbei 1:1. Somit ist ein Bestehen durch reines Theoriewissen nicht möglich. Nach Abgabe der Prüfungen werden diese korrigiert - alle Teilnehmer erhalten bei Bestehen noch am selben Tag das Ergebnis.

Aufbau – Theorieteil
Bei Multiple-Choice-Fragen können ein oder mehrere Antworten richtig sein. Offene Fragen sind mit Fließtext zu beantworten. Die Prüfungsdauer für diesen Teil beträgt 90 Minuten. Bei der Theorieprüfung sind keine Hilfsmittel erlaubt.

Aufbau – Praxisteil
Für die praktische Prüfung erhalten die Teilnehmer einen separaten VPN Zugang. Für jeden Teilnehmer existiert ein gesondertes, simuliertes Firmennetzwerk. Auf jedem System befinden sich sogenannte Flags. Diese erlangt man durch das „Hacking" von einzelnen Diensten, Gesamtsystemen oder Ähnlichem. Jede Flag kann auf mehreren Wegen erlangt werden. Der Scope wird vor Start der praktischen Prüfung mitgeteilt. Die Prüfungsdauer für diesen Teil beträgt 180 Minuten. Es sind alle technischen Hilfsmittel erlaubt.

ALLGEMEINES

Unterrichtsform:
Vollzeit in Präsenz am Standort der ProSec GmbH in Polch oder live-online

Abschluss:
Zertifikat oder Teilnahmebescheinigung

Unterrichtsdauer:
54 Unterrichtseinheiten (UE) je 45 Minuten

Video-Introduction des Lehrgangs:
https://youtu.be/VoEt4msIjC0

Unsere Dozenten:
Chris Hein, Head of Detection Service
Christian Horn, Head of Solution Service
Michael Topal, Senior PenetrationTester
Robin Unglaub, Professional PenetrationTester

Wer wir sind:
https://www.prosec-networks.com/ueber-uns/