PROFESSIONAL PENETRATION TESTER

Absolventen unseres Junior Penetration Tester (JPT) Zertifikatslehrgangs haben bewiesen, dass sie das grundlegende Handwerk des Penetration Testing bereits auf hohen Niveau beherrschen. Mit dem Professional Penetration Tester (PPT) Zertifikat können sie nachweisen, dass sie bereit sind für das nächste Level: die eigenständige Durchführung komplexer Pentests, die Mitwirkung an Red Teaming Projekten und das Anleiten von Juniors.

ZIEL & VORAUSSETZUNGEN

Ziel
Der Teilnehmer kann eigenständig Penetration Tests durchführen. Er ist in der Lage, die technische Prüfung durchzuführen und deren Ergebnisse zielgruppengerecht zu dokumentieren. Er kann eine vollumfängliche Reconnaissance durchführen und auch versteckte Angriffsvektoren identifizieren.

Er kennt die Funktionsweise von allgemeinen Sicherheitsmechanismen im Netzwerk und weiß, wie diese umgangen werden können. Weiterhin ist er in der Lage, verfügbare Exploits an die eigenen Bedürfnisse anzupassen sowie deren technische Auswirkung auf das Zielsystem einzuschätzen. Der Teilnehmer beherrscht verschiedene Methoden der Privilege Escalation und kennt die Grundlagen des verdeckten Penetration Testings (Red Teaming/OPSEC).

Der Teilnehmer ist in der Lage, technische Details einem Fachkollegen sowie dem Middle-Management in einem Unternehmen zu vermitteln. Er kann passende Lösungsvorschläge zu gefundenen Schwachstellen aufzeigen. Außerdem kann er Junioren in Projekte einbeziehen und Projekte im Team durchführen.

Voraussetzungen
Voraussetzung für den PPT ist der erfolgreich abgeschlossene JPT – alternativ Berufserfahrung als Penetration Tester mit einschlägigen Herstellerzertifikaten desselben Niveaus. Es empfiehlt sich eine abgeschlossene Ausbildung oder ein 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.

1. **Bedarfsanalyse**
   - Sizing
   - Service
   - Mögliche/Sinnvolle Prüffelder

2. **KickOff**
   - Rahmenbedingungen
   - Scoping
   - Kommunikation
   - Status
   - Prüfzeiten
   - Szenarien etc.

3. **Durchführung**
   - Information Gathering (Extern / Intern - Netzwerk / Windows)
   - Funktionsweisen & grundlegende Umgehungsmöglichkeiten von Gegenmaßnahmen (Firewalls, Loadbalancer, VLAN/ACL's, NAC)
   - Vulnerability Analysis (Automatisiert, Manuell, Gescriptet)
   - Exploitation (Kontrollierte Ausnutzung von Schwachstellen, Fuzzing, MITM, Windows Active Directory)
   - Vorbereitung eines Social Engineering Szenarios
   - Funktionsweisen & grundlegende Umgehungsmöglichkeiten von Gegenmaßnahmen (IDS, IPS, WAF, EPP/AV)
   - Post Exploitation (Privilege Eskalation, Pivoting, Lateral Movement, OPSEC Basics, Living off the Land)

4. **Abschluss**
   - Dokumentation
   - Präsentation für IT & Management

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 270 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:
64 Unterrichtseinheiten (UE) je 45 Minuten

Video-Introduction des Lehrgangs:
https://www.youtube.com/watch?v=y5kiKLvDA_Y

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/