SC305 Social Engineering Practitioner

Kurzbeschreibung:

Der Kurs **SC305 Social Engineering Practitioner** setzt mit praktischer Umsetzung und Vertiefung auf den zweitägigen SC300 Social Engineering Basics auf. Lernen Sie, wie Sie moderne Social-Engineering-Angriffswerkzeuge einsetzen, und entwickeln dadurch ein besseres Verständnis für Ihre eigenen Angriffsvektoren. Im Kurs geht es darum, sowohl **technische Skills** als **auch Soft Skills des Social Engineering** zu erweitern und so die Sicherheitsawareness im Unternehmen im Ganzen zu stärken.

Die praktischen Übungen im Kurs **SC305 Social Engineering Practitioner** umfassen den Aufbau von Fähigkeiten im Bereich der Open Source-Intelligenz (**OSINT**, **Google Dorking**), die **Technologien psychologischer Beeinflussung**, die **Risikobewertung von Menschen**, die **Verwendung von physischen Hacking-Tools**, sowie das **Entwickeln von Angriffsstrategien, basierend auf Überredung und Täuschung**.

Erweitern Sie darüber hinaus Ihr Wissen über Techniken vom **Phishing über Tailgating und Elizitieren bis zu klassischem Lock-Picking und RFID-Spoofing** mittels Flipper Zero und welche gängigen Methoden für die **Überwindung von Zutritts-, Zugangs- und Zugriffsbeschränkungen** häufig eingesetzt werden.

Im Kurspreis inkludierte Goodies:
VM für Social Engineering, **Lock-Picking-Set**, **Flipper Zero**

Zielgruppe:

- IT-Sec-Management
- Pentester
- Red- und Blueteamer

Voraussetzungen:

Vorherige Teilnahme am Kurs **SC300 Social Engineering Basics**.
Alternativ: Fundierte Grundkenntnisse im Bereich Social Engineering.

Sonstiges:

Dauer: 2 Tage

Preis: 1590 Euro plus Mwst.

Ziele:

Der Schwerpunkt der Übungen, basierend auf Erfahrungen aus der Praxis, auf dem Aufbau des Verständnisses von Angriffstechniken, mit denen SE-Pentests, aber auch reale Angriffe durchgeführt werden.

Hinweis: Im Kurs **SC305 Social Engineering Practitioner** ist das Ziel zu lernen, wie man in der Praxis Social Engineering anwendet. Dies heißt auch, hier und da die Komfortzone zu verlassen und sich in den weniger bequemen Wachstumsbereich zu wagen.

Inhalte/Agenda:

- ♦ **Lernpaket Soziale Skills und psychologische Tricks zur Manipulation von Verhalten**
- ♦ **Praxisübungen für psychologische Manipulation**
- ♦ **Aufbau eigener SockPuppets**
- ♦ **COA (Course of action) – Entwickeln eines Angriffsplans**
- ♦ **Durchführen eines Angriffs (Datenbeschaffung von vorgegebenen Zielen)**
- ♦ **Durchführen eines Spearphishings auf vorgegebenes Ziel**
- ♦ **Auswertung der Übungen**