SC305 Social Engineering Practitioner

Kurzbeschreibung:

Dieser Kurs **SC305 Social Engineering Practitioner** setzt vollständig auf die Teilnahme an dem zweitägigen SC300 Basic-Kurs auf, bevor es an Tag 3 und 4 an die praktische Umsetzung und Vertiefung geht. 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, etc), 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.

Zielgruppe:

Dieser Kurs **SC305 Social Engineering Practitioner** richtet sich an:

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

Voraussetzungen:

Niveau: Die Teilnahme an einem SC300 Social Engineering Basics innerhalb der letzten 6 Monate ist erforderlich. Ein Grundverständnis für IT ist ebenso sinnvoll, wie Softskills im Umgang mit Menschen, schließlich geht es um die Vorbereitung auf echte Social Engineering Einsätze.

Sonstiges:

Dauer: 2 Tage

Preis: 1890 Euro plus Mwst.

Ziele:

Der Schwerpunkt der Übungen, basierend auf Erfahrungen aus der Praxis und Trainings, liegt neben dem Vermitteln der grundsätzlichen ethischen und rechtlichen Rahmenbedingungen auf dem Aufbau des Verständnisses von Angriffstechniken, mit denen SE-Pentests, aber auch reale Angriffe durchgeführt werden.

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

Inhalte/Agenda:

- ♦ **Woher kommen die Gefahren, wer ist betroffen? Erstellung eines individuellen Lagebildes**
- ♦
- ♦ **Rechtliche und ethische Aspekte beim Einsatz von Social Engineering**
- ♦
- ♦ **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**
- ♦
- ♦ **Lernpakete zu folgenden Themen:**
  - ♦ ◊ Schaffung falscher Identitäten
    ◊ Recherchen im WWW via Deep Web Search, OSINT-Tools und Social Media
    ◊ Überwinden von Zutrittskontrollen und -barrieren
    ◊ Schwachstellenidentifizierung und Angriffstaktiken
    ◊ WLAN-Hacking mit verschiedenen Tools
    ◊ Hacker-USB- und LAN-Tools
    ◊ Spear-Phishing
    ◊ Vishing und Rollenspiel
- ♦ ◊
- ♦ **Auswertung der Übungen, Analyse der eigenen Angreifbarkeit und Abwehroptionen**

♦