SC305 Social Engineering Practitioner

Kurzbeschreibung:

Erlernen Sie praxisorientiert den zielgerichteten Einsatz moderner Angriffswerkzeuge sowie psychologischer Techniken. Vermittelt werden vertiefende Methoden zu OSINT, Phishing, Tailgating, Elizitieren sowie physische Verfahren wie LockPicking und RFIDSpoofing. Der Kurs legt starken Fokus auf HandsonÜbungen, dokumentierte Testabläufe und die Fähigkeit, realistische, rechtlich abgesicherte Simulationen zu planen und durchzuführen.

Zielgruppe:

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

- IT-Sec-Management
- Penetration Tester
- Red und Blue Teamer
- Sicherheitsberater und Incident Response Teams

Voraussetzungen:

Um dem Lerntempo und den Inhalten des Workshops **SC305 Social Engineering Practitioner** gut folgen zu können, empfehlen wir die vorherige Teilnahme am Kurs **SC300 Social Engineering Basics** oder gleichwertige Kenntnisse.

Sonstiges:

Dauer: 2 Tage

Preis: 1590 Euro plus Mwst.

Ziele:

- Praktische Befähigung zur Durchführung professionell dokumentierter SocialEngineeringTests (Planung, Durchführung, Reporting)
- Erlernen von OSINTMethoden inklusive sinnvoller Nutzung von KIDiensten zur effizienten und verifizierten Informationsgewinnung
- Einsatz und sichere Konfiguration von Flipper Zero in typischen Arbeitsszenarien sowie erste, sichere Programmieransätze
- Fähigkeit, in rechtlich abgesicherten Trainingsumgebungen synthetische DeepfakeSamples zu erzeugen
- Fähigkeit, autorisierte PhishingSimulationskampagnen zu planen und umzusetzen, die der Sensibilisierung und Sicherheitsvalidierung dienen
- Stärkung der persönlichen Handlungskompetenz: Teilnehmende werden durch realistische Szenarien an die Grenzen ihrer Komfortzone geführt, lernen Reflexion und Deeskalation und erhalten Methoden zur Selbstschutz und TeamNachbesprechung

Inhalte/Agenda:

- ♦ **Vertiefung sozialer Skills und psychologischer Techniken zur Beeinflussung von Verhalten**
- ♦ **Praxisübungen zu Befragungs- und Interviewtechniken (Übungen zur strukturieren Gesprächsführung)**
- ♦ **Aufbau und Betrieb glaubhafter Sockpuppets für autorisierte Tests**
- ♦ **COA (Course of Action): Erstellen und Dokumentieren von Angriffsplänen inkl. Threat Modeling und Operational Security**
- ♦ **OSINT-Workflows mit KI-unterstützten Diensten: Automatisierung, Verifikation und Quellenkritik**
- ♦ **Spearphishing Simulationen: Crafting, Delivery und Auswertung in einer autorisierten Testumgebung (Test Infrastruktur/Simulationsmailserver)**
- ♦ **Physische Übungen: Lock Picking, Tailgating Szenarien, RFID Spoofing mit Flipper Zero (Ausgabe eines Flipper Zero pro Teilnehmer; erste Anwendungsübungen und sichere Konfigurationen)**
- ♦ **SMS- und Call Spoofing: Demonstration in abgesicherter Laborumgebung, Erkennungsmerkmale und Abwehrmaßnahmen (keine unautorisierte Nutzung)**
- ♦ **Deepfake Workflow (offensive & forensische Perspektive): Erzeugen von realistischen Sprach- und Stimm-Deepfakes auf lokalen Systemen inklusive Einbindung in Meeting-Software**
- ♦ **Auswertung der Übungen: Metriken, Reporting und Empfehlungen für Stakeholder**
- ♦ **Abschluss: Erstellung eines rechtskonformen, reproduzierbaren Testplans mit Awareness und Remediation Empfehlungen**

♦