SC340 Intensivtraining - Full Scope Social Engineering

Kurzbeschreibung:

Lernen Sie, wie Sie moderne Social-Engineering-Angriffswerkzeuge einsetzen, und entwickeln Sie dadurch ein besseres Verständnis für Ihre eigenen Angriffsvektoren. Im Kurs geht es darum, vorhandene technische Skills durch Soft Skills des Social Engineering zu erweitern und so die Sicherheitsawareness im Unternehmen im Ganzen zu stärken

Die praktischen Übungen im Seminar umfassen den Aufbau von Fähigkeiten im Bereich der Open Source-Intelligenz (OSINT,Google Dorking), die Technologien der psychologischen Beeinflussung, die Risikobewertung von Menschen, die Verwendung von WLAN- und LAN-Werkzeugen, sowie die Durchführung von physischen Computerangriffen mit Keygrabbern und dem Hak5 Bash Bunny.

Erweitern Sie darüber hinaus Ihr Wissen über Techniken vom Tailgating über klassisches Lock-Picking bis zum RFID-Spoofing mittels Proxmark3 und welche gängigen Methoden für die Überwindung von physischen Zutrittsbeschränkungen häufig eingesetzt werden.

Bestandteile des Kurses sind:
Kursunterlagen, VM für Social Engineering, Lock-Picking-Set, Proxmark3 V4

Zielgruppe:

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

Voraussetzungen:

Niveau: IT-Erfahrene mit wenig bis mittlerem Social Engineering Know-How

Sonstiges:

Dauer: 4 Tage

Preis: 2850 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 für dem Aufbau des Verständnisses von Angriffstechniken, mit denen Pentests, aber auch reale Angriffe durchgeführt werden. Dadurch gewinnen Sie einen neuen Blick auf Ihre Angriffsoberfläche und sind in der Lage Sensibilisierungsprogramme für Ihren Bedarf zu optimieren und Abwehrmaßnahmen durchzuführen.

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