SC400 Hacking & Pentesting Basics

Kurzbeschreibung:

Teilnehmer lernen, wie Hacker denken und Angriffe durchführen. Im Hacking-Labor wenden sie typische Techniken praktisch an, erhalten Werkzeuge und üben deren Einsatz. Der Kurs vermittelt, wie Penetrationstests seriös geplant, umgesetzt und ausgewertet werden, um Schwachstellen systematisch aufzudecken und die Sicherheit eigener Systeme wirksam zu verbessern.

Zielgruppe:

Hacking & Penetration Testing - Basics richtet sich an IT-Fachkräfte und Spezialisten, die Vorgehensweisen, Methoden und Techniken von Hackern kennenlernen und verstehen wollen, um die Sicherheit der eigenen Systeme überprüfen sowie die Wirksamkeit eigener Abwehrmaßnahmen besser einschätzen zu können. IT-Forensikern bietet es den Blick durch die Brille des Straftäters und somit das Wissen, um Ermittlungen zielgenauer und effizienter durchführen zu können.

Voraussetzungen:

Bei unserem Workshop **SC400 Hacking & Pentesting Basics** handelt es sich um einen Basic-Kurs. Kenntnisse von IP-Netzwerken, dem WWW und gängigen Betriebssystemen sind erforderlich; vertiefte Linux- oder Windows-Kenntnisse sind nicht zwingend notwendig. Neugierde und Leidenschaft fürs Hacking sind entscheidend.

Sonstiges:

Dauer: 5 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

- Verstehen der Denkweise und Techniken von Angreifern
- Praktische Anwendung klassischer Hacking-Methoden in legalen, kontrollierten Laborumgebungen
- Fähigkeit, eigene Proof-of-Concept-Tools auf Raspberry-Basis zu konzipieren und einzusetzen (Lab-Scope)
- Einordnung und Nutzung moderner Hilfsmittel: LLMs zur Unterstützung von Recon/Phishing-Templates, KI-Tools für Webrecherche und automatisierte Pentest-Lösungen
- Kenntnis rechtlicher Rahmenbedingungen, Dokumentationspflichten und Ethical-Hacking-Standards

Inhalte/Agenda:

- ♦ **Kapitel 1**
  - ♦ ◊ Live-Hackingdemo
  - ◊ Grundlagen (the hackers view)
    - ◊ · Vom MIT-Hacker auf dem Dach bis Emotet
      · Weltkarte der Hackergruppen
      · Wie man sich nicht erwischen lässt
      · Cyber Kill Chain /Attack Matrix
      · Gesetzliche Grundlagen
      · Ethical Hacking Rules
      · Richtiges Dokumentieren
      · Wie funktionieren BugBountys
  - ◊ Open Source Intelligence
    - ◊ · Darknet, Google-Dorking, Shodan, Robtex, RIPE
      · TheHarvester, Maltego
      · Webrecherche mit KI-Tools: Nutzung von KI-Assistenten zur Priorisierung, Quellenfinder und Automatisierung von Recherchestrőmen

- ♦ **Kapitel 2**
  - ♦ ◊ Strategie und Taktik
  - ◊ Phishing /E-Mail-Attacking
    - ◊ · Grundlagen von E-Mail-Attacken
      · E-Mail-Protection (Spam/Junk/DMARC/SPF/BlackList)
      · Juristische und ethische Aspekte
      · Wir bauen ein bösartiges Makro (Conceptual)
      · Phishing -- Vishing -- Smishing
      · Phishing als Awareness-Modul
      · Einrichtung eines eigenen GoPhish-Servers
      · Erstellen von Kampagnen
      · Arbeiten mit Templates
      · Hacking mit LLMs: Einsatzmöglichkeiten von Sprachmodellen für Social-Engineering-Skripte, Template-Generierung und Automatisierungsunterstützung
  - ◊ WLAN-Hacking
    - ◊ · Klassische Techniken und Schutzmaßnahmen
      · Hacking-Tools auf Raspberry-Basis (Pwnagotchi, Björn-Images): Aufbau-Konzepte, Einsatzszenarien und Abwehrüberlegungen (hands-on Lab)
  - ◊ Man-in-the-Middle-Angriffe

- ♦ **Kapitel 3**
  - ♦ ◊ USB-Hacking
    - ◊ · USB-Ninja, BashBunny, Keylogger
      · RubberDucky /Digispark
  - ◊ Datendiebstahl durch Innentäter
  - ◊ Netzwerksniffing und -scanning allgemein
    - ◊ · Basics: ARP-Poisoning, Routing, IP-Tables, Firewalls
      · Tools: NMAP, Wireshark, eigene Raspberry-Tools (statt SharkJack)
  - ◊ Tunneling (ICMP, DNS)
  - ◊ Infection Persistence
    - ◊ · Scedule Tasks, Backdoors, Spuren verwischen
  - ◊ Automatisierte Pentest-Lösungen: Überblick über Automatisierungs-Frameworks, CI/CD-Integrationen und Orchestrierung von Scan-/Exploit-Pipelines (Konzept, Demo)

- ♦ **Kapitel 4**
  - ♦ ◊ Lateral Movement + Privilege Escalation
  - ◊ Passwortkomplexität und Angriffe
  - ◊ Einführung in Metasploit
  - ◊ Passwortcracking und Rainbow Tables
  - ◊ Web Hacking Einführung
    - ◊ · OWASP TopTen, BurpSuite, CrossSite, SQL-Injection
      · Automatisierte Web-Tests & KI-Assistenz: Einsatz automatischer Scanner, Scriptable Burp-Workflows und KI-gestützte Analysehilfen (Übersicht & Praxisbeispiele)

- ♦ **Kapitel 5**
  - ♦ ◊

- Schwachstellen in Applikationen: Buffer Overflows
- Pentesting vs. Schwachstellenscans
- Kryptografie: Zertifikate /Verschlüsselung
- Abschlusstest

- **Give-Aways / Materialien:**
- Folgende Materialien erhalten Sie zusätzlich:
  - Security-Trophies
  - Raspberry-Kit inkl. Ink-Display und fertig konfigurierter Images (Pwnagotchi / Björn) — Tool-Bausatz für eigene LAN/WLAN-Prototypen
  - DigiSpark mit Demo-Payloads
  - Kali-Linux-VM, Cheat-Sheets und Skripte
  - Dauerhafter Zugang zu Linkplattform mit über 300 Services und Tools
  - Zertifikat
  -