SC400 Hacking & Pentesting Basics

Kurzbeschreibung:

Teilnehmende 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:

Dies ist ein Basic-Kurs. Sie benötigen zwar Kenntnisse von IP-Netzwerken, dem WWW und gängigen Betriebssystemen, Sie müssen aber weder Linux- noch Windows-Crack sein. Sie wissen was ein Virenscanner ist und haben einen IT-Security-Hintergrund. Vor allem aber benötigen Sie eine Leidenschaft und Neugierde auf das Hacken.

Sonstiges:

Dauer: 5 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Sie verstehen die Denkweise und grundlegende Techniken von Hackern und können diese in einfachen Penetrationstests mit verschiedenenTools anwenden. Sie werden anschließend in der Lage sein, Kali-Linux, den DigiSpark und den SharkJack bei Hacking-Demos zu verwenden. Gleichzeitig lernen Sie auch die rechtlichen Grundlagen und das Arbeiten eines seriösen Pentesters kennen.

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
  · Cyberkillchain /Attack Matrix
  · gesetzliche Grundlagen
  · Ethical Hacking Rules
  · richtiges Dokumentieren
  · Wie funktionieren BugBountys
  ◊ Open Source Intelligence
  ◊ · Darknet, Google-Dorking, Shodan, Robtex, Ripe
  · TheHarvester, Maltego

- ♦ **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
  · Phishing -- Vishing -- Smishing
  · Phishing als Awareness-Modul
  · Einrichtung eines eigenen GoPhish-Servers
  · Erstellen von Kampagnen
  · Arbeiten mit Templates
  ◊ WLAN-Hacking
  ◊ 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, SharkJack
  ◊ Tunneling (ICMP, DNS)
  ◊ Infection Persistence
  ◊ · Scedule Tasks, Backdoors, Spuren verwischen

- ♦ **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

- ♦ **Kapitel 5**
- ♦ ◊ Schwachstellen in Applikationen: Buffer Overflows
  ◊ Pentesting vs. Schwachstellenscans
  ◊ Kryptografie: Zertifikate /Verschlüsselung
  ◊ Abschlusstest

- ♦ **Folgende Give-Aways erhalten Sie zusätzlich:**
- ♦ ◊ Security-Trophies
  ◊ SharkJack mit Payloads
  ◊ Digispark mit Payloads
  ◊ Kali-Linux-VM, Cheat-Sheets und Skripte
  ◊ Zertifikat
- ♦ ◊