SC420 Hacking & Pentesting Advanced

Kurzbeschreibung:

Teilnehmende sammeln praxisnahe Angriffserfahrungen in einem Greybox-Szenario: Von der initialen Kompromittierung bis zur Kontrolle des Domain–controllers wird ein kompletter Angriff durchgespielt. Der Kurs bietet darüber hinaus Einführungen in Recherchen auf Darknet-Marktplätzen/Foren zur Beschaffung von Tools der dunklen Seite, Einsatz von spezialisierten LLMs zur Entwicklung von Zero-Day-Exploits und Angriffsstrategien.

Zielgruppe:

Der Kurs **SC420 Hacking & Pentesting Advanced** wendet sich an Administratoren, Pentester und Security-Professionals mit bereits fundierten Hacking-Erfahrungen; geeignet als Vorbereitung für operative Zertifizierungen (z. B. OSCP) und als Aufbau innerhalb der qSkills™-Modulreihe.

Voraussetzungen:

Um den Inhalten und dem Lerntempo des Kurses **SC420 Hacking & Pentesting Advanced** gut folgen zu können, empfehlen wir folgende Vorkenntnisse:

- Gute Kenntnisse in Windows/Active Directory und Linux-Umgebungen
- Erfahrungen mit Penetrationstests oder entsprechende Vorkenntnisse empfohlen
- Vertrautheit mit Skriptsprachen (PowerShell, Bash, C/C) von Vorteil

Sonstiges:

Dauer: 5 Tage

Preis: 3350 Euro plus Mwst.

Ziele:

- Tiefergehendes Verständnis von Penetrationstest-Methodik in realistischen Greybox-Szenarien
- Fähigkeit, Recon- und Exploitation-Workflows nachvollziehbar, dokumentiert und rechtssicher durchzuführen
- Sensibilisierung für neue Bedrohungsbilder (Darknet-Ökonomie) und Einordnung, wie Organisationen damit umgehen sollten
- Kompetentes Nutzen von KI-Unterstützung für defensive Analysen, Automatisierung und Priorisierung — bei gleichzeitiger Einhaltung ethischer und rechtlicher Vorgaben
- Erlernen von Erkennungs-, Forensik- und Härtungsmaßnahmen nach komplexen Angriffsszenarien

Inhalte/Agenda:

- **Rahmenthemen und ethische Aspekte**
  - ◊ Gesetzlicher Rahmen für Penetrationstests
  - ◊ Haftungsfragen und Vertragsgestaltung
  - ◊ Ethische Richtlinien und Best Practices
  - ◊ Protokollieren und Empfehlungen erarbeiten

- **Recon und Informationsbeschaffung**
  - ◊ OSINT-Techniken (Open Source Intelligence)
  - ◊ Netzwerk-Scanning und Enumeration
  - ◊ Schwachstellenanalyse aus der Ferne
  - ◊ Darknet-Marktplätze - Funktionsweise, typische Geschäftsmodelle, Erkennungsmerkmale, Risiken für Organisationen
  - ◊ Einsatz spezialisierter KI/LLM-Modelle zur Unterstützung offensiver Workflows

- **Einführung in das Szenario**
  - ◊ Vorstellung der Ziele und Rahmenbedingungen
  - ◊ Arbeiten mit Metasploit und Cobalt Strike (autorisiert, kontrolliert)
  - ◊ Überblick über verfügbare Tools und Ressourcen

- **Initiale Kompromittierung**
  - ◊ IBitLocker-Konfigurationen analysieren (defensiv & forensisch)
  - ◊ Techniken zur Erlangung lokaler Admin-Rechte (Exploit-Analyse, Patch-Assessment, Privilege-Escalation-Methoden in Prüfungsumfang)
  - ◊ Deaktivierung von Sicherheitslösungen: Erkennungswege, EDR-Bypass-Mechanik aus Sicht von Detection & Response

- **Post-Exploitation und Laterale Bewegung**
  - ◊ Vertieftes Netzwerk-Scanning und Enumeration
  - ◊ Lateral Movement-Techniken und deren Erkennung (Pass-the-Hash, Kerberoasting, AS-REP Roasting)
  - ◊ Angriffe auf AD / EntraID und andere IAM-Komponenten — Erkennung, Härtung, Monitoring
  - ◊ Persistenz-Mechaniken: Erkennen, Bereinigen, Forensik

- **Windows- und Linux-Server-Hacking**
  - ◊ Privilege Escalation in heterogenen Umgebungen
  - ◊ Techniken zur Erlangung von Domänen-Admin-Rechten — Verteidigungs- und Erkennungsmaßnahmen
  - ◊ Vorbereitung und Abwehr von Golden-Ticket-Angriffen (forensische Analyse, Detektion, Risikominderung)

- **Finale und Nachbereitung**
  - ◊ Durchführung (Demonstration im Lab) und Beobachtung der Angriffsabläufe
  - ◊ Bereinigung, Spurenfeststellung und forensische Nacharbeit
  - ◊ Empfehlung zur Härtung und Verteidigung

- **Abschlussbesprechung**
  - ◊ Diskussion der verwendeten Techniken
  - ◊ Empfehlungen zur Härtung und Verteidigung
  - ◊ Reflexion über ethische Implikationen und rechtliche Konsequenzen

- **Spezielle Ergänzungen**
  - ◊ Darknet-Marktplätze Verständnis der Ökonomie, typische Produkte/Services, Indikatoren für Beschaffung/Vertrieb
  - ◊ Spezialisierte LLMs & KI-Modelle (Einsatz im Verteidigungs- und Forschungsrahmen): Überblick über Nutzungsszenarien wie automatisierte Recon-Summaries, Priorisierung von Schwachstellen, Generierung sicherer Testskripte für autorisierte Labs, sowie Governance- und Sicherheitsanforderungen beim Einsatz. Deutliche Abgrenzung: kein Training oder Einsatz zur Entwicklung oder zum Abbau von Zero-Day-Exploits; Fokus auf verantwortungsvolle Anwendung, Validierung, und Responsible Disclosure-Prozesse
  - ◊ Threat Intelligence & Responsible Vulnerability Research zum Umgang mit gefundenen Exploit-Information, Prozesse zur Verifikation, Meldung an Hersteller, rechtliche Absicherung und Zusammenarbeit mit Behörden

  - ◊