SC420 Hacking & Pentesting Advanced

Kurzbeschreibung:

Realistische Angriffserfahrungen zu sammeln, ist für angehende Whitehats eine echte Herausforderung. Dieser Kurs **SC420 Hacking & Pentesting Advanced** ist eigens dafür konzipiert, anhand eines typischen Greybox-Angriffs die Eskalation von der initialen Kompromittierung bis zur absoluten Kontrolle durchzuspielen und dabei verschiedene Tools auszuprobieren. Nach den notwendigen theoretischen Grundlagen bekommt jeder Kursteilnehmer einen ausgeschalteten unbekannten Computer übergeben, um darüber Stück für Stück einen Angriff bis hin zum Domaincontroller durchzuführen.

Zielgruppe:

Dieser Kurs **SC420 Hacking & Pentesting Advanced** wendet sich an Administratoren und Pentester, welche bereits über Erfahrungen im Hacking verfügen und eine operative Zertifizierung wie etwa OSCP anstreben.

Der Kurs ist gut als Einleitung oder Fortsetzung der weiteren qSkills Modulkurse des Redteam Skills geeignet:

- **SC415 EC-Council Certified Ethical Hacker (CEH Elite)**
- **SC355 Open Source Intelligence (OSINT) Practitioner**
- **OT300 OT Pentesting**

Voraussetzungen:

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

- Die Teilnehmer sollten gute Kenntnisse in Windows und Active Directory-Umgebungen haben
- Eine vorherige eindringliche Testerfahrung wäre ein Bonus
- Vertrautheit mit C, C- und PowerShell wäre ebenfalls vorteilhaft, aber nicht notwendig.

Sonstiges:

Dauer: 5 Tage

Preis: 3350 Euro plus Mwst.

Ziele:

Der Kurs **SC420 Hacking & Pentesting Advanced** zielt darauf ab, den Teilnehmern ein umfassendes Verständnis der rechtlichen und ethischen Grundlagen von Penetrationstests zu vermitteln, einschließlich der Haftungsfragen und besten Praktiken. Zusätzlich soll den Teilnehmern praktisches Wissen über Recon- und Informationsbeschaffungstechniken nahegebracht werden, wie OSINT und Netzwerk-Scanning, um

Schwachstellen aus der Ferne zu analysieren. Der Kurs fördert die Fähigkeit zur initialen Kompromittierung von Systemen, einschließlich BitLocker-Umgehung und dem Erlangen von Admin-Rechten, sowie Techniken zur Deaktivierung von Sicherheitslösungen. Ein weiteres Ziel ist es, den Teilnehmern Methoden der Post-Exploitation und lateralen Netzwerkbewegung beizubringen, einschließlich der Angriffe auf Active Directory und weitere Identity-Management-Systeme. Abschließend sollen die Teilnehmer in der Lage sein, komplexe Angriffe wie den Golden Ticket-Angriff durchzuführen, während sie zugleich Strategien zur Bereinigung und Verschleierung von Angriffsspuren erwerben und verbessern.

Inhalte/Agenda:

- **Rechtliche Grundlagen und Recon**

- ♦ **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
- ♦ ◊
- ♦ **Einführung in das Szenario**
  - ♦ ◊ Vorstellung der Ziele und Rahmenbedingungen
    ◊ Arbeiten mit Metasploit und Cobalt Strike
    ◊ Überblick über verfügbare Tools und Ressourcen
- ♦ ◊

Initiale Kompromittierung

- ♦ **BitLocker-Verschlüsselung umgehen**
  - ♦ ◊ Analyse der BitLocker-Konfiguration
    ◊ Anwendung von TPM-Sniffing-Techniken
    ◊ Extraktion des Volume Master Key (VMK)
- ♦ **Erlangen lokaler Admin-Rechte**
  - ♦ ◊ Ausnutzung von Schwachstellen im Betriebssyste
    ◊ Privilege Escalation-Techniken
    ◊ Umgehung der User Account Control (UAC)
- ♦ ◊
- ♦ **Deaktivierung der Sicherheitslösung**
  - ♦ ◊ Analyse installierter Sicherheitssoftware
    ◊ Techniken zum Umgehen und Deaktivieren von Antivirus und EDR
    ◊ Umgang mit Windows Defender, AMSI und AppLocker
- ♦ ◊

Post-Exploitation und Laterale Bewegung

- ♦ **Laterale Bewegung im Netzwerk**
  - ♦ ◊ Vertieftes Netzwerk-Scanning und Enumeration
    ◊ Ausnutzung von Schwachstellen in Netzwerkdiensten
    ◊ Pass-the-Hash und andere Lateral Movement-Techniken
- ♦ ◊
- ♦ **Angriffe auf Active Directory,EntraID und andere IAM**
  - ♦ ◊ Enumeration der AD-Struktur
    ◊ Bruteforce-Angriffe auf Exchange, VNC SSH und RDP
    ◊ Ausnutzung von Fehlkonfigurationen
    ◊ Kerberoasting und AS-REP Roasting
- ♦ ◊
- ♦ **Persistenz etablieren**
  - ♦ ◊ Einrichten von Backdoors
    ◊ Erstellen versteckter Admin-Accounts
    ◊ Manipulation von Gruppenrichtlinien
- ♦ ◊

Windows- und Linux-Server-Hacking

- ♦ **Privilege Escalation in LDAP und AD-Domäne**
  - ♦ ◊ Ausnutzung von Berechtigungsfehlern in Linux-Servern
    ◊ Techniken zur Erlangung von Domänen-Admin-Rechten
    ◊ DCSync-Angriffe
    ◊ Ausnutzung von Vertrauensstellungen zwischen Domänen
- ♦ ◊
- ♦ **Vorbereitung des Golden Ticket-Angriffs**
  - ♦ ◊ Extraktion des krbtgt-Hashes
    ◊

◊ Erstellung und Verwendung gefälschter Kerberos-Tickets
- ♦ ◊

Finale und Nachbereitung

- ♦ **Durchführung des Golden Ticket-Angriffs**
  - ♦ ◊ Erzeugung des Golden Tickets
  - ◊ Demonstration der vollständigen Domänenkontrolle
- ♦ ◊
- ♦ **Bereinigung und Verschleierung**
  - ♦ Löschen von Spuren und Logs
  - ♦ Entfernen von Hintertüren und bösartigen Konfigurationen
- ♦

Abschlussbesprechung

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