SC401 Hacking & Penetration Testing - RedTeam BlueTeam Special

Kurzbeschreibung:

Lernen Sie von erfahrenen WhiteHats wie Angriffe ablaufen. Sie erhalten einen Einblick in die Welt des Hackens und verstehen Absichten und Vorgehensweisen von Angreifern. Sie erfahren durch praktisches Anwenden im Hacking-Labor, mit welchen Techniken Hacker arbeiten. Sie erhalten von uns Werkzeuge und lernen diese in Blueteam- und Redteam-Operations einzusetzen. Nutzen Sie die gewonnenen Kenntnisse, um die Sicherheit Ihrer eigenen Systeme zu überprüfen. Sie lernen, worauf es bei simulierten Attacken ankommt, wie sie seriös durchgeführt werden und wie man die Ergebnisse effizient nutzt.

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 Angriff und Verteidigung und können diese in einfachen Penetrationstests mit verschiedenen Tools erkennen und 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:

- Die Motivation und Methodik der Angriffe
  - Der grundsätzliche Unterschied zwischen Angreifer und Verteidiger
  - Script Kiddies, Hacktivisten, Nation State Actors und kommerzielle Hacker – was sind deren Motive und Methoden
  - Der Ablauf von Angriffen dargestellt auf der Lockheed Martin Cyber Kill Chain
  - verschiedene Weiterentwicklungen der Cyber Kill Chain (z.B. IPC CKC)

- Werkzeuge von Hackern
  - Vorstellung von Werkzeugen und Workarounds in den Themenfeldern der CKC:
    - 1. Recon: OSINT-Tools, Pretexting, Shodan, Ripe, Robtex, Social Media, Intelligence, Google-Dorking
    - 2. Bewaffnung: Auxiliary, Skripting, Code Scrambling, Conter Antivirus, Makros
    - 3. Zustellung: Scanning mit NMAP, Phishing/Vishing/Smishing/DeepFake
    - 4. Exploiting: Ausnutzung von Schwachstellen mit LOLBas, Makros, JavaScript-Exploits
    - 5. Installation: Lateral Movement, Privilege Escalation mit Hashdump, Mimkatz und Bloodhound, Logcleaning, Backdoors
    - 6. Verbindung zum Comand&Control-Server über HTTPS, RDP, SSH, ICMP-Tunneling oder DNS-Tunnel (z.B. Iodine)
    - 7. Action on Objectives: Ransomwareattacken, Exfiltration, Spionage und Sabotage

- Malware: Von Viren bis Rootkits
  - Viren, Trojaner, Würmer, Rootkits und was dahintersteckt

- Sniffing: Angriffe, Man-in-the-Middle-Angriffe, LAN- Angriffe, WLAN-Angriffe
  - Wo und wie funktionieren diese Angriffe und welche Schwachstellen werden hier ausgenutzt?
  - Missbrauch von Protokollen
  - jedes Protokoll hat seine Schwäche: 802.X ebenso wie http oder DNS – wir beleuchten die Ausnutzbarkeit von Schwächen.

- Informationsbeschaffung: Reconnaissance und Enumeration
  - wir kennen nun bereits verschiedene Tools, jetzt trainieren wir das Information Gathering

- Auskundschaften von Netzwerke
  - Wireshark und NMAP, aber auch Traceroute, Netstat und ARP helfen beim Erkunden von Netzwerken
  - Probe und Beacon ermöglichen WLAN-Attacken mit Spidern. Aber was ist ein Evil Twin?

- Portscan
  - von paranoid bis aggressive kann ein Portscan unauffällig oder regelrecht laut und spürbar sein
  - welche Standardports gibt es (im Application Level Gateway)

- Fingerprinting
  - Identifizieren von Anwendungen auf Webservern
  - welche Informationen lassen sich wie erbeuten / ausnutzen?
  - Welche Informationen liefern Fehlermeldungen und Versionsinformationen?

- Vulnerability Checks
  - Wie entstehen Schwachstellen und wie lassen sie sich vermeiden?
  - die Geschichte von CVE und CVSS
  - Greenbones OpenVAS oder Tenables Nessus: Wie setzt man Schwachstellenscanner ein?
  - Shodan Monitor und Security Scorecard für die Sicht der Angreifer

- Exploitation mit Metasploit
  - Auxiliary, Exploits, Payloads und Posts
  - Training mit Metaspoit in unserer Proxmox-Umgebung sowohl gegen Windows als auch Linux

- Kennwortangriffe
  - Spoofing statt Cracking – wie es am besten funktioniert
  - Warum Kennwort, wenn der Hash genügt? Wie funktioniert PasstheHash
  - Angriff O365 Auth mit 2FA-Bypass mittels EvilGinx (MiM-Framework)
  - Crackingmethoden und ihre Geschichte am Beispiel von NTLM
  - Auslesen lokal verfügbarer Passworthashes mit Hashdump und JohntheRipper oder Crackstation
  -

- ◊ Arbeiten mit Mimikatz und Bloodhound auf der Jagd nach dem Golden Ticket

- Digitale ◊ Forensik – Methoden
- ◊ Sichern -> Analysieren -> Bewerten = Grundlagen der IT-Forensik
  ◊ Unterschied zwischen Liveforensik und Deadforensik
  ◊ Logkollektoren, SIEM, Locard-Prinzip und rechtliche Grundlagen

- Speicherung ◊ von Angriffsspuren
- ◊ Einsatz forensischer Werkzeuge in der IT-Triage
  ◊ Umgang mit flüchtigen und nichtflüchtigen Speichern
  ◊ Sichern von Prozessorcache und Arbeitsspeicherinhalten
  ◊ Sichern von physischen und virtuellen Datenträgern und deren Untersuchung

- Analyse ◊ von Sicherheitsvorfällen
- ◊ die Bedeutung der Timeline und warum sind NTP-Server so wichtig
  ◊ Auswertung von Spuren auf dem Host und im Netzwerk
  ◊ Gründliche Analyse oder schnelle Wiederherstellung? Bereinigung vs Neuinstallation
  ◊ Grenzen der Analyse
- ◊