

kukE 290-3 - Metasploit Framework auf einer Backtrack/Kali-Linux Plattform

Dieser Praxisworkshop baut direkt auf die erworbene Zertifizierung zum Certified Ethical Hacker (CEH) des EC-Council auf und bietet die Gelegenheit, anhand vorbereiteter Szenarien das Eindringen in Geräte und Infrastrukturen unter Verwendung des Metasploit- Frameworks durchzuführen. Der Praxisanteil beträgt hierbei circa 80%; die vermittelte Theorie bezieht sich hauptsächlich auf kurze Erläuterungen der Funktion durchgeführter, spezieller Angriffe (wie etwa die Rolle von NOPs 0x90-Prozessorbefehlen im Zusammenhang mit BufferOverflows), während diese ausgeführt werden. Ziel des Workshops ist es, den Teilnehmer in die Lage zu versetzen, dass im CEH erworbene Wissen effektiv und mit ausgesuchten, praxisnahen Werkzeugen anwenden zu können. Die Angriffe erfolgen vom MSF auf einer Backtrack/Kali-Linux-Plattform aus.

Seminarinhalt:

- Einführung in das Metasploit-Framework (MSF)
- Grundlagen und Bedienung
- Aktive und passive Aufklärung mit dem MSF
- Das Exploitation-Modul
- Angriffe auf Server
- Angriffe auf Endgeräte (Clients)
- Payloads (Malwaretransport auf die Zielsysteme)
- Einsatz des Meterpreters
- Aufrechterhaltung eines dauerhaften Zugriffes
- Weiterführende Konzepte

Seminarübersicht:

- Dauer: 2 Tage
- Preis: 1.950,00 €
- Uhrzeit: 9:00 - 17:00 Uhr
- Seminarunterlage: Lab-Guide

Empfohlene Vorkenntnisse: Ausbildung zum Certified Ethical Hacker (CEH) oder vergleichbare Kenntnisse

Zielgruppe: Revision, IT-Sicherheitsbeauftragte, Systemadministratoren

Standorte: Frankfurt

Termine & Anmeldung:

kukE 290-3 - Metasploit Framework auf einer Backtrack/Kali-Linux Plattform

<https://seminare.edc.de/seminardetails/kukfe-290-3-metasploit-framework-auf-einer-backtrackkali-linux-plattform/>