



Metasploit Einführung & Aufbau

Vermittlung des Theorie- und Praxiswissens für den effizienten Einsatz des Metasploit Frameworks und für die Anpassung und Entwicklung von Exploits

Listenpreis

3.500,00 € exkl. MwSt

4.165,00 € inkl. MwSt

Dauer

5 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin



Manuela Krämer

Leitung
Informationssicherheit

Kontakt/Fragen:

m.kraemer@cbt-training.de

Telefon: +49 (0)89-4576918-12

Inhalte

Modul 1 Metasploit Einführung

- **Vermittlung des Theorie- und Praxiswissens für den effizienten Einsatz des Metasploit Frameworks (MSF)**
 - Übersicht und Architektur des Metasploit Frameworks
 - Bezugsmöglichkeiten und kommerzielle Varianten
 - Einrichtung und Schnittstellen
 - Möglichkeiten auf Basis der enthaltenen Module und Tools
 - Bedienung und Einsatz
 - Fallbeispiel
- **Einführung**
- **Metasploit-Framework und -Pro**
 - Übersicht und Struktur des Frameworks
 - Besonderheiten innerhalb KALI
- **Architektur und Bestandteile**
 - Philosophie
 - Modultypen
 - Schnittstellen
 - Erweiterungen
- **Bedienung und Befehle**
 - Hilfe zur Selbsthilfe
 - CLI Kommandos
 - Grafische Benutzeroberfläche
 - Modulooptionen
- **Job- und Sessionmanagement**
 - Möglichkeiten
 - Nutzung
- **Datenmanagement**
 - Anbinden und Nutzen einer Datenbank
 - Verzeichnisstruktur
- **Payloads**
 - Shells



- Reverse-Shells
- Commands
- Post-Exploitation
- Standalone Payloads
- **Sondermodule**
 - Generic Listener
 - Breakpoint
- **Ausführliches Fallbeispiel Workshop**
 - Metasploitable 3

Modul 2 Metasploit Aufbau

- **Vermittlung des Praxiswissens für die Anpassung und Entwicklung von Exploits**
 - Hinweise zum Labor
 - Weitere Werkzeuge
 - Praktischer Einsatz der Werkzeuge
 - Kombinieren des Werkzeugeinsatzes
 - Fallbeispiele mit steigendem Schwierigkeitsgrad
- **Grundlagen**
 - Rechnerarchitektur und Speichermanagement
 - Debugger inkl. Plugin
 - Maschinensprache und Assembler
- **Metasploit-Tools**
 - pattern_create und pattern_offset
 - nasm_shell
 - msfvenom
- **PoC-Entwicklung**
 - Grundlagen Python
 - Befehle und Kontrollstrukturen
 - Verstehen von fertigen PoC's
 - Entwickeln neuer Exploits
 - Zusammenarbeit in der Community
- **Metasploit Module**
 - Grundlagen Ruby
 - Variablen
 - Klassen und Methoden
 - Befehle und Kontrollstrukturen
 - Verstehen bestehender Module
 - Anpassen von Modulen
 - Konvertieren von "Fremd"-Exploits
 - Entwickeln eigener Module
 - Zusammenarbeit in der Community
- **Fallbeispiele**
 - Einsatz von Metasploit
 - Fallbeispiel



Ziele

Das Modul 1 erklärt Architektur und Bedienung von Metasploit anhand zahlreicher, praktischer Übungen.

Im Modul 2 zeigt der Referent fortgeschrittene Möglichkeiten von Metasploit genauso wie Ansätze zur Automatisierung und Individualisierung auf.

Zielgruppe

- Zukünftige Penetrationstester
- Mitarbeiter aus Administration, Netzwerk und SOC
- Mitarbeiterausbildung für IT-Security
- Strafverfolgungsbehörden und Angehörige von Cyber-Defense/Offense Einheiten
- alle, die sich für Metasploit interessieren

Voraussetzungen

Dieses Seminar beschäftigt sich in zwei Schritten mit dem Metasploit Framework in KALI Linux.

Kursvoraussetzungen:

- **Professional Security Expert**
 - Penetrationstest Grundlagen Theorie
 - Vorgehensmodelle Pentesting
 - Umgang mit Linux / Kali Linux
 - Kenntnis und Anwendung wichtiger Kali Tools
- **Hilfreich:**
 - Betriebssystemkenntnisse (MS Windows, Linux, etc.)
 - Sicherheitsbewusstsein ((C)ISO, SiBe, Penetrationstester, Administrator, etc.)
 - Weiteres IT-Wissen (Programmierung, Netzwerke, Web-Technologie, etc.)