



Wissen, wie es geht

WORKSHOP

Windows Hacking kompakt

In diesem Workshop vermitteln wir einen Überblick zu Angriffsstrategien auf Windows Umgebungen mit Fokus auf Accounts und Microsoft Active Directory. Gemäß dem Motto „Lernen durch Hacking“ werden Angriffe an der vorhandenen Umgebung des Kunden mit den Administratoren gemeinsam durchgeführt, ausgewertet und Abwehrmaßnahmen empfohlen. Um den Workshop an Ihre Bedürfnisse anzupassen, erfolgt vorab grundsätzlich eine Bestandsaufnahme Ihrer AD-Umgebung. Die Teilnehmer:innen erleben eine anschauliche und kompakte Verknüpfung von Theorie & Praxis und können optional auch selbst Angriffe durchführen.

Den Umfang des Workshops bestimmen Sie: Wählen Sie Basic oder Advanced

Anforderungen BASIC 1. Tag

- ▶ Einsatz einer Microsoft Windows Domain und grundlegendes Verständnis Microsoft Active Directory
- ▶ Raum mit Beamer und Netzwerkzugriff

Anforderungen ADVANCED optionaler 2. Tag

- ▶ LDAP Account mit Adminrechten an einem Server und Client
- ▶ Kenntnisse von Authentifizierungsprotokollen sind wünschenswert
- ▶ PC im Unternehmensnetzwerk

Nutzen

- ✓ Härtung des internen Netzwerks gegenüber Angriffen
- ✓ Entwicklung eines gemeinsamen Fahrplans zur Härtung des Netzwerkes
- ✓ Sensibilisierung der Administratoren gegenüber Angriffen



Regelmäßige Pen-Tests zeigen, dass in mittelständischen Unternehmen zu 90% keine Härtung des Microsoft Active Directorys durchgeführt wird. Im Workshop zeigen wir, wie Cyberkriminelle diese Lücke als Einfallstor in Ihre IT-Systeme nutzen.

DAVID HÄNTZSCHEL, PENETRATION TESTER

Inhalte des Workshops



BASIC | 1. Tag

Kompakte Vermittlung aktueller Angriffsszenarien in Windows-basierten Netzwerken und der geeigneten Abwehrmöglichkeiten.

- **Angriffe auf Microsoft Windows Umgebungen (mit Live-Demo)**
- **Information Gathering**
- **Protokolle & Angriffsszenarien (u.a.):**
 - › Credential Harvesting
 - › Pass-the-hash
 - › NTLMv2 Relay
 - › Angriffe auf Service-Accounts
- **Auswertung und Zusammenfassung**

Der Workshop ist für 7 h inkl. Pausen konzipiert.



ADVANCED | optionaler 2. Tag

Die Grundlagen aus dem ersten Tag werden live an der IT-Umgebung Ihres Unternehmens veranschaulicht. Dazu setzen wir gemeinsam eine virtuelle Arbeitsumgebung auf, um die besprochenen Angriffsvektoren bei Ihnen zu prüfen.

Ergänzend zu den Themen des 1. Tages betrachten wir u.a. Folgendes:

- **AD-Berechtigungen**
- **Scan nach offenen Dateifreigaben**
- **Knacken von Zugangsdaten**
- **Auswertung und Diskussion der Befunde**

Der Workshop ist für 8 h inkl. Pausen konzipiert.

Ihre Trainer



Christian Müller

Principal Technology Consultant



Certified Information
Systems Security Professional



Certified Cloud
Security Professional

EC SA

EC-Council Certified Security Analyst



David Häntzschel

Senior System Engineer

**PENETRATION
TESTER**

EC SA

EC-Council Certified Security Analyst
v10

SHD bietet ganzheitliche Lösungen für Ihre Informationssicherheit an:

Schulungen für User
(u.a. eLearning)
und Administratoren

Technische
IT-Sicherheitskonzepte
(u.a. Netzwerk-Security)

Security-Lösungen
für Core, DMZ
und Edge-Bereich

SIEM-Lösungen

Kontinuierliches
Schwachstellen-
Management

Prozessorientiertes
Informationssicher-
heitsmanagement

IT-Security Check

Individuelle
Penetration Tests

Security Operations Center als Managed Service

SHD ist seit 1990 erfolgreich am Markt und betreut über 650 Kunden deutschlandweit in den Bereichen Digitalisierung, Informationssicherheit, Infrastruktur, Managed Services und IT-Service-Management.



SHD ist zertifiziert
nach ISO 9001
und ISO 27001

SHD Kurzporträt

- 1990 in Dresden gegründet
- 160 Beschäftigte
- 42,4 Mio. EUR Umsatz 2021
- Stammhaus in Dresden, Geschäftsstellen in Berlin, Leipzig, Hamburg, Nürnberg und in der Lausitz
- Kunden aus Industrie-, Krankenhaus- u. Bankbereich sowie aus öffentlichen Einrichtungen

Geschäftliche Schwerpunkte

- IT-Infrastruktur Services
- Informationssicherheit
- Managed und Cloud Services
- IT-Management
- Digitalisierung von Prozessen

Kontakt

SHD.
info@shd-online.de
www.shd-online.de

