

Kerberos ist ein verteilter Authentifizierungsdienst für offene und unsichere Computernetze, der von Steve Miller und Clifford Neuman basierend auf dem Needham-Schroeder-Protokoll zur Authentifizierung (1978) entwickelt wurde.

### Ihr Nutzen

Nach dem Seminar verstehen Sie die Kerberos Architektur, können Service-Principal Names Verwalten und die verschiedenen Arten von Kerberos Delegation einrichten. In vielen praxisorientierten Beispielen erlernen Sie die Einrichtung und Fehlersuche innerhalb von Kerberos in Windows Netzwerken.

### Preis pro Teilnehmer

EUR 1550,- exklusive der gesetzlichen MwSt.

### Seminardauer

2 Tag(e)/Day(s)

### Seminarinhalte

#### 1. Tag

##### \* Grundlagen

- Authentifizierung vs. Autorisierung
- Grundlagen Windows Security Konzept
- Access Tokens und Access Control Lists
- NTLM vs. Kerberos

##### \* Was ist Kerberos?

- Ursprung und Historie
- Aktuell: Kerberos v5
- Das Ticket und seine Verwendung
- Ticket Granting Service (TGS)
- KDC, TGT und Key Requests, Ticket LifeTime
- Service Principal Names
- Windows Werkzeuge
- Hands-On-Lab: Tickets & SPN
- Netzwerk-Tracing des Kerberos Traffics

#### 2. Tag

##### \* Delegation

- Basic Delegation vs. Constrained Delegation
- Resource-Based Constrained Delegation

##### \* Real World Szenarios

- Beispiel: Multi-Tier Delegation
- From Client to Webservice to Database

##### \* Fehlersuche und Troubleshooting

- Auswirkungen des Domain-Modes
- Event-Logging und Debugging

##### \* Group Policy Settings for Kerberos

##### \* Kerberos Erweiterungen

- Claim Based Authentication
- Flexible Authentication Secure Tunneling (FAST)
- Compound Authentication
- Kerberos Armoring
- KDC Proxy

### Voraussetzungen

Kenntnisse von Active Directory, Grundkenntnisse von Authentifizierung

### Hinweise

Version: 2022

