

Securing Active Directory

Teil 2: Absicherung durch das Unternehmenszugriffmodell

In diesem Kurs steht die Sicherheit des Active Directory im Vordergrund. Wer schon mal etwas von Programmen wie Mimikatz und Co. gehört hat, weiß, dass eine Active Directory Umgebung nicht vor Angriffen geschützt ist. In diesem Kurs lernen Sie grundlegende Dinge über das Protokoll Kerberos sowie über die Berechtigungsvergabe kennen und erfahren, wie Sie eine lokale Infrastruktur absichern können. Dieser Kurs eignet sich ebenfalls für Teilnehmer des Kurses Active Directory Fundamentals & LDAP, um das gewonnene Grundwissen rund um das Active Directory abzurunden.

Kursinhalt

- Funktionsweise des Kerberos-Protokolls
- NTLM, Kerberos Delegations und klist
- Active Directory Gruppen und das Kerberos-Protokoll
- Berechtigungen im Active Directory vergeben
- Einrichtung von Dynamic Access Control (DAC)
- Erläuterung des Tier Modells
- Authentication Policies & Silos
- Privileged Access Manager (PAM), Bastion Forests & Shadow Principals
- Local Administrator Password Solution (LAPS)
- Managed Service Accounts
- Fine Grained Password Policies

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Der Kurs eignet sich für fortgeschrittene und erfahrene Active Directory Administratoren.

Voraussetzungen

Die Teilnehmer sollten zuvor den Kurs Active Directory Fundamentals & LDAP – Struktur, Einrichtung und Verwaltung besucht haben.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.ch/go/ADS2

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland		2 Tage CHF 2.195,-
Online Training		2 Tage CHF 2.195,-
Termin/Kursort		Kurssprache Deutsch
15.05.-16.05.25 Online	23.10.-24.10.25 München	
10.07.-11.07.25 Hamburg	23.10.-24.10.25 Online	
10.07.-11.07.25 Online	11.12.-12.12.25 Frankfurt	
28.08.-29.08.25 Düsseldorf	11.12.-12.12.25 Online	
28.08.-29.08.25 Online		

Stand 07.05.2025



Inhaltsverzeichnis

Securing Active Directory – Teil 2: Absicherung durch das Unternehmenszugriffmodell

- 1 Kerberos**
 - 1.1 Ablauf**
 - 1.1.1 Authentication Service Request
 - 1.1.2 Authentication Service Response
 - 1.1.3 Ticket-Granting Service Request
 - 1.1.4 Ticket-Granting Service Response
 - 1.1.5 Application Server Request
 - 1.1.6 Application Server Response
 - 1.1.7 Zusammenfassung
 - 1.2 Klist**
 - 1.3 Access Token**
 - 1.4 Cross-Realm Access**
 - 1.5 Kerberos Pre-Authentication**
 - 1.6 Zugriff über IP-Adressen**
 - 1.7 Delegation**
 - 1.7.1 Unconstrained Delegation
 - 1.7.2 Constrained Delegation
 - 1.7.3 Resource Based Constrained Delegation
 - 1.7.4 Konfiguration
 - 1.8 Übung**
- 2 Gruppen**
 - 2.1 Berechtigungsvergabe über Gruppen**
 - 2.2 Group Scopes**
 - 2.2.1 Domain Local
 - 2.2.2 Global
 - 2.2.3 Universal
 - 2.3 Berechtigungsvergabe**
 - 2.3.1 Beispiel
 - 2.4 Group Type**
 - 2.5 Konfiguration**
 - 2.5.1 Scope und Type
 - 2.5.2 Mitglieder
 - 2.5.3 Mitglied von
 - 2.5.4 Primäre Gruppe
 - 2.6 Übung**
- 3 Berechtigungen**
 - 3.1 Arbeiten mit Rechten**
 - 3.1.1 Gewähren
 - 3.1.2 Verboten
 - 3.1.3 Freigaben
 - 3.1.4 Übung
 - 3.2 Delegieren**
 - 3.2.1 Wizard
 - 3.2.2 Attribute
 - 3.2.3 Übung**
 - 3.3 Dynamic Access Control**
 - 3.3.1 Unterstützung aktivieren
 - 3.3.2 Attribute definieren
 - 3.3.3 Claims
 - 3.3.4 Resource Properties
 - 3.3.5 Central Access Rule
 - 3.3.6 Central Access Policy
 - 3.3.7 Gruppenrichtlinie
 - 3.3.8 Policy auswählen
 - 3.3.9 Classification Rule
 - 3.3.10 Übung
 - 4 Zugriffe absichern**
 - 4.1 Administrative Ebenen**
 - 4.1.1 Tier 0
 - 4.1.2 Tier 1
 - 4.1.3 Tier 2
 - 4.1.4 Weitere Systeme
 - 4.2 Authentication Policies & Silos**
 - 4.2.1 Klassische Einstellungen
 - 4.2.2 Authentication Policies
 - 4.2.3 Claims
 - 4.2.4 Bedingung
 - 4.2.5 Rubriken
 - 4.2.6 Authentication Silos
 - 4.2.7 Voraussetzungen
 - 4.2.8 Anmeldung**
 - 4.2.9 Vergleich**
 - 4.2.10 Übung
 - 4.3 Managed Service Accounts**
 - 4.3.1 Group Managed Service Accounts
 - 4.4 Privileged Access Management**
 - 4.4.1 AD Feature
 - 4.4.2 Vertrauensstellung
 - 4.4.3 Shadow Principal
 - 4.4.4 Admin-Konto
 - 4.4.5 Temporäre Mitgliedschaft
 - 4.4.6 AES-Verschlüsselung
 - 4.4.7 Übung
 - 4.5 Kennwortrichtlinien**
 - 4.5.1 Klassische Einstellungen
 - 4.5.2 Fine Grained Password Policies
 - 4.6 Local Administrator Password Solution**
 - 4.6.1 OU und Gruppe anlegen
 - 4.6.2 Installation auf dem DC
 - 4.6.3 Schema Erweiterung**
 - 4.6.4 Berechtigungen**
 - 4.6.5 Softwareverteilung**
 - 4.6.6 Konfiguration**
 - 4.6.7 Gruppenrichtlinie aktualisieren**
 - 4.6.8 Verwaltungstools**
 - 4.6.9 Übung**

