Kerberos 101

How Kerberos works and how to configure it in complex authentication scenarios

This 1 or 2-day level 300 course explains how Kerberos authentication works in simple and complex scenarios. Also covered are the benefits in terms of security between Kerberos and NTLM.

Key benefits

- Why did Microsoft implement Kerberos
- What are the differences and advantages compared to NTLM
- How to configure Kerberos for simple authentication
- How to configure Kerberos Delegation
- Troubleshooting authentication problems
- What happens after the authentication?

Syllabus

- Overview about Kerberos
- Kerberos Components
- Logon scenarios using Kerberos
- Differences between NTLM and Kerberos
- Delegation, Constrained Delegation and Protocol Transition by example (SQL, IIS)
- Identifying and troubleshooting Kerberos issues

Overview

Kerberos is the standard authentication protocol since Windows 2000. To really make use of this protocol it is vital to understand some key components and to make sure these components are configured correctly. This workshop introduces into the Kerberos protocol and all key components and describes common configurations. In the 2-day version of this class attendees can configure typical Kerberos scenarios as well as troubleshoot common problems.

TARGET AUDIENCE
This workshop is intended for system engineers, system administrators, consultants and developers who support or develop Kerberos enabled applications and services.

BUSINESS NEEDS
Kerberos offers a lot more features than NTLM. The downside is that under some circumstances Kerberos has to be configured in order to operate correctly. This workshop explains how the protocol works and talks about common configurations and best practices.

Pre-Requisites

Participants should have a good understanding in administering a Windows Server environment. Experience in Active Derisory and Internet Information Server is required (Visual Studio is beneficial for the labs but not a requirement)