>> Windows Server Deep Dive

Server Hardening, Security

EGOS! the education company

Aktuelle Versionen von Windows beinhalten viele Funktionen um die Angriffsfläche auf ein System zu reduzieren. Services, Ports, Shares, Kennwörter sind ein klassiches Angriffsziel.

Ihr Nutzen

Nach diesem Workshop kennen Sie die unterschiedlichen Techniken um ein System gegen Angriffe abzusichern und können Baselines für verschiedene Rollen im System aufbauen und anwenden.

Voraussetzungen

Windows Administrationskenntnisse

Preis pro Teilnehmer

EUR 960,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

Version: 2012 R2

Seminarinhalte

1. Tag
* Überblick - Windows Server 2008 R2 Security
- Sicherheitstechniken in Windows 2008 R2
- Änderungen in Authentifizierung & Autorisierung
- Sicherheit und Virtualisierung
- Server Core, Read-Only Domain Controller (RODC)
* Windows Server Sicherheitskomponenten
- Übersicht über die Windows 2008 R2 SSPs
- Local und Domain-Logon
- Negotiate, NegoEx, Kerberos und NTLM
- Winlogon, Netlogon, Credential Providers
- Security Internals, Password, Sam etc.
* Sicherheitslücken, Hacking
* Password
- Wann und wo wird ein Password genutzt?
- LM Hash und NT Hash
- Credential Cache
- Benutzer-und Maschinen-Password
- Cracken von Passwörtern (Local, Domain)
- Password-Richtlinien
* Secure Channel & Computerpassword
- Aufbau des Secure Channels
- Maschinenpassword und Session Key Negotiation
- Testen des Secure Channels
- "Broken" Secure Channel - Reset Secure Channel
- Ändern des Computerpasswords

2. Tag
* Neue Sicherheitstechniken
- Windows Firewall with Advanced Security (WFAS)
- Host-Firewall und AuthIP Erweiterung mit User Authentication
- Firewall Profile: Domain, Privat, Public
- Inbound & Outbound Rules
- IPSec Domain Isolierung
* Server Service Hardening
- Service Konten: LocalSystem, LocalService, NetworkService
- Service Control Manager (SC)
- Service Security – SID & Privilegien
- Access Token
- SVCHOST-Prozess und Dienste
- Service SID Type: Unrestricted und Write-Restricted
- Service Isolation
- Einschränken der Zugriffe und Privilegien von Services
* Analysieren & Absichern
- Security Policy - Security Configuration Wizard (SCW)
- Analysieren der Serverinstallation mit SCW, Scwcmd und MBSA
- Security Templates für Windows Server 2008
- Security Configuration & Analysis (SCA)
- Role-Based Policies
- Erzeugen der Sicherheitsrichtlinien für GPO
* Monitoring & Auditing
* Auditing
- Überwachungsrichtlinien
- Advanced Audit Policy, Audit Category und Subcategory
- Auditpol.exe
- Auswerten der Sicherheitsereignisse mit PowerShell V2
* Windows Server 2008 R2 Sicherheitsrichtlinien
- Lokale und Gruppenrichtlinien
- Empfohlene Sicherheitsrichtlinien für Windows Server 2008
- Import & Export von Sicherheitseinstellungen
- Geeignete OU-Struktur für Windows Server - Gruppenrichtlinien
- AppLocker (2008 R2)