Windows Server - Implementing and Administering Security

Course code: GOC175

What we teach you We will familiarize you with the security principles on Windows platform We will explain the details of clients´ accounts running, their SID and the principles of authentication using Kerberos to you You will learn and you will try how trust relationships between domains and forest are running You will learn how to work with client groups correctly and how to optimise their use You will learn to administer NTFS and Share permissions in detail, ABE and script its setting and live in environment with UAC You will learn how to manage the membership in local groups and how to delegate the administration to the lower administrators You will start to use security principles in Group Policy effectively You will familiarize with Windows Firewall and you will learn to administer it effectively and safely with the minimum operation opening You will introduce AD CS certificate authority and you will distribute certificates You will run encrypt communication using IPSec and you will learn how to manage computer access to network using 802.1x You will introduce SSL certificates for IIS web server and other services as SQL Reporting Services You will encrypt disk partitions by BitLocker and set the key recovery through Active Directory You will protect the file access using EFS and certificates You will run remote access using VPN (PPTP, L2TP i SSTP) and you will also run DirectAccess and Remote Desktop Gateway You will make the remote access safe through NAP and you will introduce strict health policiesRequired skills The knowledge of the courses stated in Previous courses and Related courses Windows Server 2008/R2 administration and basic function of Active Directory TCP/IP and DNS technology basis Basic rules of security such as certificates, encrypting, verification and managing of accessTeaching methodsLectures and practical examples, exercises on the virtual computers on the Hyper-V platform.
Teaching materials GOPAS own study materials in electronic or printed form
Course Outline Windows security subsystem Users and service accounts, logon session, access token, SID and SID history Users authentication, authentication by NTLM, Kerberos, SSL certificates and chip cards Auditing, access monitoring and verification Multi-users environment, process identities, service identities and IIS AppPoolIdentity, SYSTEM, Network Service and Local Service Trust, forest trust, trust accounts, selective trust and complex environment, users migration NTFS and Share permission, user rights, Access Based Enumeration (ABE) User Account Control (UAC) Local groups, delegation of permission for server and station administration, delegation in Active Directory Group Policy and Security Policy, software restrictions, password policies Windows Firewall and its central administration through Group Policy Active Directory Certificate Services (AD CS), PKI and certificates and private keys administration Network access, IPSec and 802.1x encrypting TLS/SSL certificates and their application for IIS, Reporting Services, TS Gateway etc. BitLocker and EFS encrypting and their differences, application and back up of keys Remote access VPN - PPTP, L2TP, SSTP, DirectAccess, Remote Desktop Gateway (TS Gateway) Network Access Protection (NAP) and NPS

What we teach you

- We will familiarize you with the security principles on Windows platform
- We will explain the details of clients´ accounts running, their SID and the principles of authentication using Kerberos to you
- You will learn and you will try how trust relationships between domains and forest are running
- You will learn how to work with client groups correctly and how to optimise their use
- You will learn to administer NTFS and Share permissions in detail, ABE and script its setting and live in environment with UAC
- You will learn how to manage the membership in local groups and how to delegate the administration to the lower administrators
- You will start to use security principles in Group Policy effectively
- You will familiarize with Windows Firewall and you will learn to administer it effectively and safely with the minimum operation opening
- You will introduce AD CS certificate authority and you will distribute certificates
- You will run encrypt communication using IPSec and you will learn how to manage computer access to network using 802.1x
- You will introduce SSL certificates for IIS web server and other services as SQL Reporting Services
- You will encrypt disk partitions by BitLocker and set the key recovery through Active Directory

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- You will protect the file access using EFS and certificates
- You will run remote access using VPN (PPTP, L2TP i SSTP) and you will also run DirectAccess and Remote Desktop Gateway
- You will make the remote access safe through NAP and you will introduce strict health policies

Required skills

- The knowledge of the courses stated in Previous courses and Related courses
- Windows Server 2008/R2 administration and basic function of Active Directory
- TCP/IP and DNS technology basis
- Basic rules of security such as certificates, encrypting, verification and managing of access

Course Outline

- Windows security subsystem
- Users and service accounts, logon session, access token, SID and SID history
- Users authentication, authentication by NTLM, Kerberos, SSL certificates and chip cards
- Auditing, access monitoring and verification
- Multi-users environment, process identities, service identities and IIS AppPoolIdentity, SYSTEM, Network Service and Local Service
- Trust, forest trust, trust accounts, selective trust and complex environment, users migration
- NTFS and Share permission, user rights, Access Based Enumeration (ABE)
- User Account Control (UAC)
- Local groups, delegation of permission for server and station administration, delegation in Active Directory
- Group Policy and Security Policy, software restrictions, password policies
- Windows Firewall and its central administration through Group Policy
- Active Directory Certificate Services (AD CS), PKI and certificates and private keys administration
- Network access, IPSec and 802.1x encrypting
- TLS/SSL certificates and their application for IIS, Reporting Services, TS Gateway etc.
- BitLocker and EFS encrypting and their differences, application and back up of keys
- Remote access VPN - PPTP, L2TP, SSTP, DirectAccess, Remote Desktop Gateway (TS Gateway)
- Network Access Protection (NAP) and NPS

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk