Windows Server - Active Directory SAE, Tiering and Red Forest

Course code: GOC159

The three-day course is intended for administrators and architects of IT infrastructure built on Active Directory and Azure Active Directory, who want to learn how user accounts security works, how to properly handle privileged administrator accounts, how to securely manage the entire on-prem and hybrid environment to avoid compromising administrator credentials, and thus either completely preventing, or at least isolating incidents such as ransomware and other today's infections, for example, preventing the entry and survival of APT.

Who is the course designed for?

- The course is intended for administrators and architects of security and IT infrastructure primarily built on Active Directory (AD DS) and Azure Active Directory (AAD)

What will you learn by taking this course?

- You will learn to understand against what types of attacks the principles of UAE, tiering and red forest are appropriate
- You will learn to understand the basic security principles of Active Directory and Azure Active Directory, the security of their accounts and groups/roles, replications and passwords, and access control within these directories
- You will learn to understand their ability to isolate or completely restrict the entry of malware in general and ransomware, spyware, APT (advanced persistent threats) in particular and their further spread
- You will learn to understand how security measures such as LDAPS, Kerberos Armoring, Kerberos Compound ID, Protected Users group work, how to minimize the use of NTLM and how to secure the credentials of privileged accounts
- You will learn how to set up a SAE (secure administrative environment) for the management of AD DS, servers and workstations, Azure AAD, Office 365 and other as well as foreign cloud services and other systems such as network elements, printers, etc.
- You will learn why is tiering needed and how to implement it and effectively separate privileged administrator accounts, how to use smart cards and other multi-factor authentication methods (MFA - multi factor authentication)
- You will learn how to enable convenient supervising for IT admins and suppliers in such an environment
- You will learn why forest is a security boundary, how all domains in it are compromised and why is it appropriate to run multiple separated forests, for example for DMZ and so on
- You will learn how and why to implement red forest for multi-forest environments

Required skills

- Knowledge in extent of the courses which are listed in the bellow sections Previous Courses and Related Courses
- Good understanding of TCP / IP and DNS technologies

Course outline

- Examples of attacks we want to defend against
- Spyware, ransomware, keyloggers, password managers risks
- Risks of stored login data, risks of weak passwords, risks of (non) locked accounts
- SSO injections (single sign on), impersonation risks, Kerberos delegations risks and Kerberos protocol transition
- Risks associated with Enterprise AD CS (certification services) and issuance of login certificates into smart cards (smart card logon)
- Compromised Domain Admin accounts are compromising the entire forest
- Possibilities of deploying multifactor authentication, smart-card logon (PKINIT), TPM virtual chip cards, tokens, Azure MFA usage
- Accounts and groups with rights and access at the Domain Admins level, or with the ability to elevate to this level
- Principles of AD DS and Azure AD account and password synchronization, federation services (AD FS) authentication for Office365, and Kerberos pass-through authentication for Azure

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

- Access control within AD DS LDAP and Azure AD, AdminSDHolder, LDAP permissions
- Access control to Group Policy and Intune management and the risks and protections associated with it, plus Advanced GPM
- DNS security and DHCP dangers
- Multi-domain environments, forest trust, and authentication of user accounts and secure use of groups between them
- Identification of tier0 (DC) devices and privileged administrator accounts
- Identification of tier1 (servers) devices and privileged administrator accounts
- Identification of tier2 (endpoint) devices and privileged administrator accounts
- Isolation of tier0-tier1-tier2 privileged administrator accounts using User Rights Assignment, Kerberos Authentication Policies, Selective Authentication
- Use of Windows Firewall or Private VLAN technologies to break individual security zones (tier)
- Building a secure administrative environment (SAE)
- Technology and appropriate security measures for jump servers (JS), privileged access workstations (PAW) and privileged access management servers (PAM)
- Access and its protection on JS, PAW and PAM, security of administrators' login data in such an environment, access via VPN and temporary or permanent access
- Foreign suppliers
- Identity integration (IDM) and red-forest scenarios for multiple domain environments, separate forests for DMZ and other isolated networks, OT and production networks built on Windows.

Preparation for certification exams

- Most Microsoft certification exams do not require students to attend an official MOC course in order to pass the exam. This applies to all certifications except for MCM
- Official Microsoft MOC courses as well as our own GOC courses are good ways of preparation for Microsoft certifications such as MCP, MTA, MCSA, MCSE or MCM
- This does not mean that official MOC courses would serve as the only necessary preparation. The primary goal of an MOC course is to provide for sufficient theoretical knowledge and practical experience to effectively work with the related product
- MOC courses usually cover most of the topics required by their respective certification exams, but often do not give every topic the same amount of time and emphassis as may be required to successfully pass the exam

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