PV176 Správa systémů MS Windows II

Jaro 2016

Libor Dušek

Autentizační protokol Kerberos

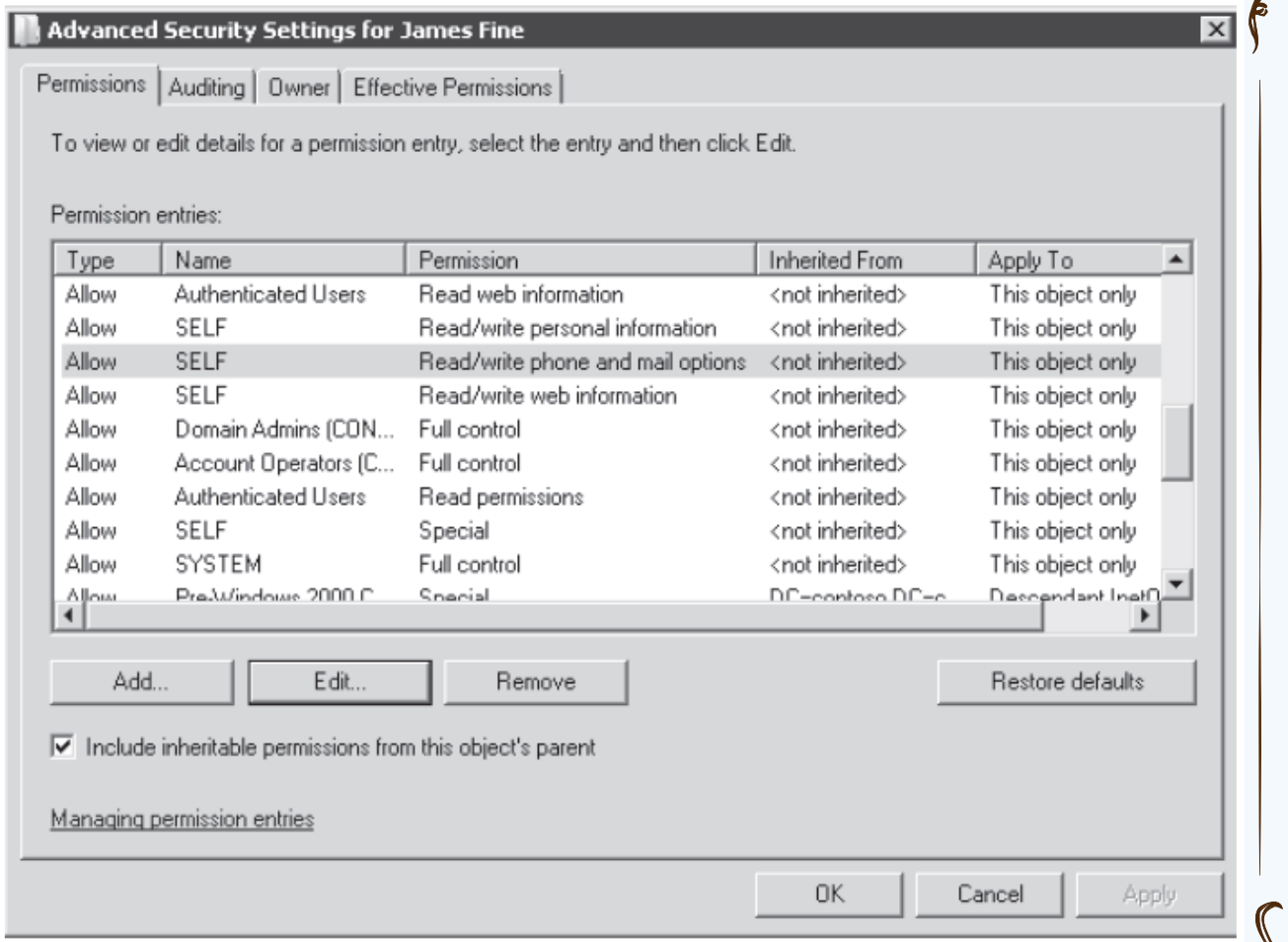
- Pro autentizaci v rámci AD se ve výchozím nastavení používá protokol Kerberos, z kompatibilních důvodů je k dispozici i NTLM (+NTLMv2).
- Když se klient pokouší přihlásit (pomocí Kerberos), je autentizační požadavek poslán DC – komponentně KDC (Key Destribution Center).
  - Po ověření identity získá klient od KDC **TGT** (Ticket-Granting Ticket)

Autentizační protokol Kerberos 2

- K přístupu na jiný (než jeho lokální) počítač (nicméně stále v rámci stejné domény) potřebuje získat **session ticket**.
    - Klient zašle KDC svůj TGT (jako důkaz, že už byl autentizován a není potřeba to dělat znovu) spolu s informacemi kam potřebuje získat přístup (počítač + služba). KDC ověří, že se jedná o stejnou doménu a zašle zpět příslušný session ticket.
    - Klient se následně přihlásí na danou službu a předloží session ticket. Server ověří, že je ticket validní.
    - Ověřování = klasické použité kryptografie.
- Z uvedeného plyne, že server **neprovádí autentizaci uživatele** ale pouze akceptuje informace z DC.
- Zjednodušený popis – podrobně ve studijních materiálech – 09_Kerberos.pdf

Delegace oprávnění

- Umožnit ostatním uživatelům upravovat objekty v AD
- Proč?
  - Více administrátorů, každý má zodpovědnost za určitou oblast
  - Rutinní úlohy jako je restartování hesel, odemknutí účtu lze delegovat na technickou podporu, vedoucí oddělení nebo nejchytřejšího člověka hned za administrátorem = úspora času, rychlejší reakce… / automatizace = princip nejmenších nutných oprávnění.



DACL princip

Obrázek z MSTraining kit 70-640

Delegace oprávnění 2

- Příklad: Potřebujeme umožnit všem uživatelům z oddělení technické podpory aby mohli restartovat uživatelská hesla
  - přidat oprávnění na změnu hesla skupině „help desk“ pro jednotlivé účty?
  - přidat oprávnění na změnu hesla skupině „help desk“ pro OU, ve kterém jsou umístěny uživatelské účty?
- Dědění oprávnění v OU: „include inheritable permissions from this object’s parent“
  - Například uživatelská skupina nemůže zdědit oprávnění „reset password“, protože nemá atribut password

Delegace oprávnění 3

- Umístěním všech uživatelských účtů do OU *People* můžeme jednoduše delegovat oprávnění pro restart hesla lidem z oddělení technické podpory
- Umožňuje jednoduše delegovat další oprávnění pro všechny uživatelské účty zároveň:
  - úprava adresy, jména, pracovního zařazení, atd.
  - vytváření nových účtů

Úkoly – Delegace oprávnění

1. Prohlédněte si v Active Directory Users and Computers, záložku security nějakého uživatelského účtu např. „Pepa“
   - Aktivujte [View – Advanced Features] a prohlédněte si jej znovu
2. Vytvořte si OU „People“ a přemístěte do ní uživatele „Pepa“. Vytvořte nového uživatele, který je členem pouze skupiny Domain Users a znáte jeho heslo. Vytvořte už. skupinu Help Desk.
3. Na kartě Security pro uživatele Pepa, přidejte skupině Help Desk oprávnění Reset Password.
4. Spusťte MMC konzoli jako uživatel Help Desku– můžete resetovat heslo uživateli „Pepa“? [vypnout UAC, pridat Pepu do Print Operators]
5. Zkuste upravit jiný údaj uživatele „Pepa“ a resetovat heslo jiným uživatelům.
6. Použijte nástroj Delegate Control, pro delegování oprávnění reset hesla a odemknutí účtu skupině Help Desk.
   1. Vytvořte MMC Snap-In, který bude obsahovat tlačítka (odkazy) pro reset hesla a odemknutí účtu a umožní už. skupině Help Desk provádět tyto aktivity na OU „People“.

Delegace oprávnění – jak na to?

- Kdo má vytvářet uživatelské účty?
  - HR zadá požadavek na IT „vytvořte uživatele X, pozice Y“ -> IT vytvoří a zařadí do skupin.
    - Ve skutečnosti: HR potřebuje zařadit do nějakého personálního systému (zákonná evidence, účetnictví…) -> rovnou může (program) vytvářet uživatele v AD ve správných skupinách.
  - Do jakých skupin, jaká oprávnění má mít uživatel?
    - Zpravidla: „X bude dělat to stejné co Y“
    - HR ale nemůže vědět jaká všechna oprávnění má Y, případně kam všude má Y přístup (má skupina „file server“ přístup do složky osobními údaji nebo ne?)
    - Hromadění oprávnění, v případě povýšení/ponížení musí někdo revidovat oprávnění.
  - Jeden z možných přístupů: **Role Based Access Control**

Úkoly – RBAC

- Finanční údaje firmy jsou udržovaný ve 2 systémech
  - **Účetní systém** je tvořen 2 sdílenými složkami, jedna na serveru A, druhá na serveru B
  - **Datový sklad** je tvořen DB v SQL Serveru (pro simulaci využijeme jinou sdílenou složku na serveru A)
- S finančními údaji mají pracovat následující osoby:
  - Asistentka – zadává údaje do účetního systému
  - Vedoucí kanceláře – zadává údaje do účetního systému, provádí hromadné exporty
  - Obchodní analytik – převádí data z účetního systému do datového skladu ve kterém se provádí automatizované výpočty
  - Obchodník – prostřednictvím aplikace přistupuje k datovému skladu a zobrazuje data
  - Majitel firmy požadujeme úplný přístup ke všem zdrojům
- Nahvrněte řízení přístupu pomocí **RBAC**, dodržujte princip **AGDLP**

Read Only Domain Controller – RODC

- Zvláštní typ DC, databáze je pouze pro čtení
- Pro nasazení v pobočkách, kde nelze plně zajistit fyzickou bezpečnost a odpovídající správu
  - Credential Caching
  - Uložení hesla pro účet uživatele/počítače
- Lze definovat pro jaké účty bude heslo ukládáno
- Je možné definovat „lokálního administrátora“ RODC, který není členem Domain Admins
- Forest Functional Level (FFL) alespoň 2003, alespoň jeden DC WS2008

Zabezpečení DC obecně

- Security Configuration Wizard (SCW)
  - Deaktivuje nepotřebné služby (pomocí politik), nastaví FW pravidla, nabídne šifrování SMB a LDAP provozu, aktivuje audit policy
  - Depracated - Microsoft Security Compliance Manager
- Auditování událostí – velikost logu v závislosti na počtu dnů uchování události, automatické zpracování událostí vs. manuální.
- SYSKEY – klíč chránící data v AD Data Store (např. hashe už. hesel)
  - Ve výchozím nastavení je klíč uložen lokálně – fyzický přístup ke stroji tedy znamená i přístup k SYSKEY
  - Password startup – klíč je chráněn heslem, které je nutno zadat při startu DC
  - Store SYSKEY on floppy disk –celý klíč je umístěn na externím zařízení, nutno vložit při startu

Zabezpečení DC obecně 2

- Administrátor musí být důvěryhodná osoba, použijte adekvátní množství nástrojů pro ověření „kvality“. Např. registr dlužníků, trestní rejstřík, důsledně ověřené reference.
- Admin. oprávnění pouze pro administrátory, pro všechny ostatní dodržovat princip nejmenších nutných oprávnění – delegování.
  - Administrátoři by měli používat minimálně 2 účty pro správu -> běžný (na emaily, filmy, office práci atd.), privilegovaný (pouze na správu). [Kde všude zadáváte a ukládáte svoje heslo?]
- Přejmenovat výchozí uživatele Administrator (a jeho popis), vytvořit „falešného“ a monitorovat pokusy o přihlášení pod těmito uživateli.

Zabezpečení AD obecně

- Všichni autentizovaní uživatelé mají „Add workstations to domain“ privilegium. Pomocí atributu ms-DS-MachineAccountQuota je regulován počet stanic, které mohou připojit do domény (výchozí nastavení je 10).
  - Takto vytvořený účet počítače je možné „zneužít“ viz http://myitpath.blogspot.com/2010/05/creating-infinite-semi-anonymous.html
- Aktualizace počítačů/serverů – ideální stav: probíhá automaticky, centralizovaný reporting (kdo má nainstalovaný hotfix atd.), nestahuje z internetu ale lokálního serveru: WSUS (Windows Server Update Services)

Zabezpečení AD Password policies

- Comp Conf – Win Settings – Security Settings
- Account Policies
  - Password Policy – požadavky na hesla (Default Domain Policy)
  - Account Lockout Policy – podmínky zamknutí účtu v případě opakovaného nesprávného zadání hesla
- Local Policies
  - Audit Policy – nastavení logování událostí
  - User Rights Assignment – speciální oprávnění
- Security Options – co se jinam nevešlo
- Fine Grained Policy – WS2008: možnost definovat různé požadavky na složitost hesla pro uživatele/skupiny

Zabezpečení AD prakticky

- Pozor na skupiny:
  - Authenticated Users
  - Domain Users
  - Domain Computers
  - Users
  - Everyone
- Např. Users obsahuje Authenticated Users = naprosto všichni uživatelé ve všech trusted doménách.
- Proto nepoužívejte v nastavení Security – ideálně nikde, náhrada:
  - All = všichni živý uživatelé z dané domény (bez servisních a dalších bulit-in účtů)

A co dál?

- Fyzická bezpečnost zařízení?
  - Nejenom krádež ale i zálohované napájení, konektivita, náhradní díly,
- Co nebo kdo je nejslabší článek zabezpečení?
- Postupy a nástroje, které vám pomohou z pravidla existují – používejte je.

Úkoly

1. Jaké informace může o sobě měnit sám uživatel (ve vlastnostech už. účtu) ve výchozím nastavení?
2. Podívejte se na nástroje http://technet.microsoft.com/en-us/security/cc297183:
   - Microsoft Security Compliance Manager
   - Microsoft Baseline Security Analyzer
   - Enhanced Mitigation Experience Toolkit (EMET)