PŘÍSTUPOVÁ PRÁVA A PRÁCE S HESLY

AUTENTIZACE (OVĚŘENÍ) UŽIVATELE

- způsob ověření identity uživatele v systému za účelem řízení přístupu k systému či zdrojům
- nejčastěji užívanou autentizační metodou je autentizace důkazem znalostí, tedy například znalostí hesla
- autentizace důkazem vlastnictví (bezpečnostní předmět, čipová karta)
- autentizace důkazem vlastností (biometrické metody - otisk prstu, obraz sítnice)

SILNÉ HESLO

- kombinaci s číslicemi a jinými znaky (velká, malá písmena, speciální znaky, ? ! / (_ % > apod.)
- heslo by také mělo mít alespoň 10 znaků, lépe 12
- vyvarovat se jménům, datům narození a podobným osobním údajům
- hesla pravidelně měnit
- Hesla u všech uživatelských účtů v počítači
- Dobře zapamatovatelné (nepsat si ho třeba na monitor)

JAK VYTVOŘÍME SILNÉ HESLO PŘ.

- silné heslo vytvoříte tak, že si pro sebe řeknete dobře zapamatovatelnou frázi
- např. Moje Mladší Sestra Se Jmenuje Veronika
- mezi první (nebo poslední) písmena slov vložte číslice (třeba poslední dvojčíslí roku vašeho narození)
- na začátek (nebo kamkoli jinam) vložte speciální znak
- heslo potom je: !M8m5SsJ?V
- heslo by nemělo obsahovat písmena s diakritikou a většinou ani mezery

ŘÍZENÍ PŘÍSTUPU

- Řízení přístupu je proces, při kterém je ověřována míra oprávnění a uživatelských práv k přístupu ke zdrojům. Ověřují se uživatelé, skupiny uživatelů i počítače.

HASH

- **většina lepších systémů neukládá hesla uživatelů, ale pouze jejich otisk (hash)**
- **hash je vypočtený řetězec vždy stejné délky, který se vypočítá ze zadaného textu, zpětně se text z hashe zjistit nedá**
- **po zadání vašeho hesla z něj systém vytvoří hash a ten porovná se svým dříve uloženým hashem**

The quick brown fox jumps over the lazy dog =

9e107d9d372bb6826bd81d3542a419d6

ODCIZENÍ HESLA

- heslo může být odcizeno:
- sociotechnickými prostředky, tj. podvodem zjištěno od uživatele
- využitím neopatrnosti uživatele – heslo je napsané na lístečku nalepeném na monitoru, na spodní straně podložky pod myš, …
- pomocí keyloggeru – malware běžící na počítači, který zjišťuje zápisy znaků do políček heslo a odesílá je uživateli
- stejná hesla – uživatelé často používají stejná hesla na důležité i méně důležité operace
- např. heslo na e-mail jde přes Internet v případě protokolu POP3 zcela nezašifrováno

ZJIŠTĚNÍ (PROLOMENÍ) HESLA

- útok hrubou silou (brute force attack)
  - výkonný počítač zkouší všechny možné kombinace znaků, přičemž začíná omezenou skupinou možností (zvládne miliony hesel za vteřinu)
  - kombinací je možné vytvořit P^N, kde N je počet znaků hesla a P je počet znaků, ze kterých vybíráme
  - např. ze 4 číslic je možné vytvořit 10^4 hesel, tj. 10000 kombinací
  - u hesla dlouhého 6 znaků vytvořené z 200 znaků (ASCII obsahuje 256 znaků) je kombinací 200^6, tj. 64 000 000 000 000 kombinací

ZJIŠTĚNÍ (PROLOMENÍ) HESLA

- slovníkový útok
  - útočník zjistí jazyk uživatele kterého chce napadnout
  - použije kompletní slovník daného jazyka a začne zkoušet slovo po slovu, nejlépe podle jejich četnosti používání
  - běžné jazyky používají cca 200 000 slov, často používaných je cca 10 000
  - slova se zkoušejí i pozpátku a nebo se za ně přidávají číslice

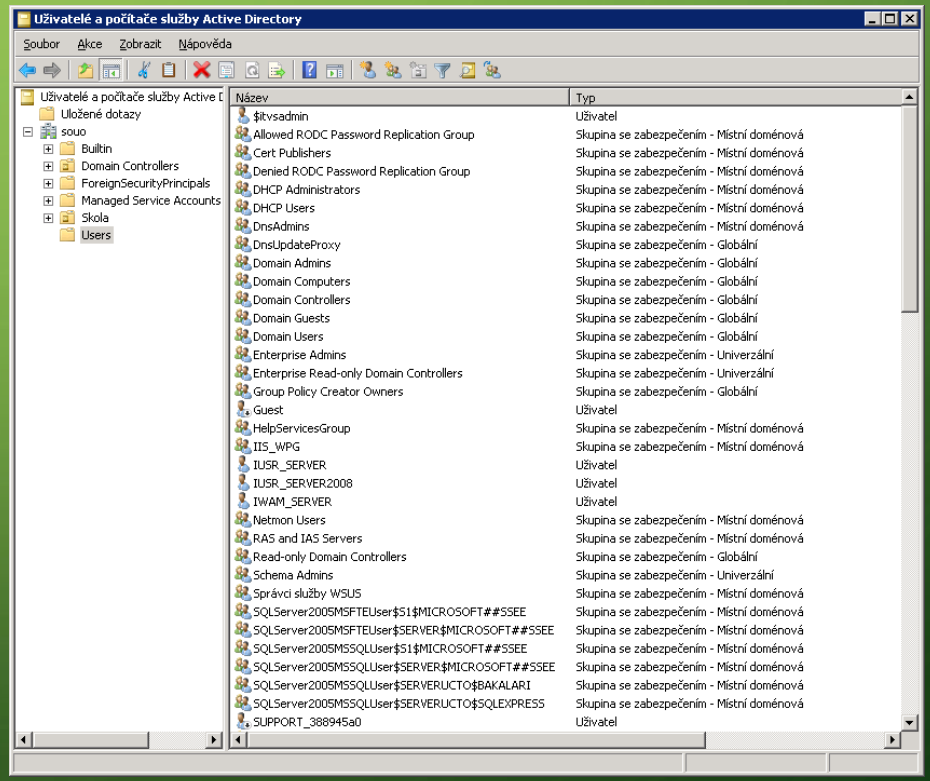
PŘÍSTUPOVÁ PRÁVA

- **Nastavení správných práv a oprávnění v OS (Windows) patří mezi základní nástroje zabezpečení sdílených prostředků.**
- **Uživatelské účty s přidělením oprávnění**

UŽIVATELSKÉ ÚČTY

- Lokální
  - Guest
  - User
  - Administrator
- Doménové
  - User
  - Power User
  - Domain Administrator, Backup Operators, …

Uživatelské skupiny, např.



OPRÁVNĚNÍ KE SDÍLENÍ, PŘÍSTUPU KE SDÍLENÉ SLOŽCE/SOUBORU V DOMÉNĚ (SERVER)