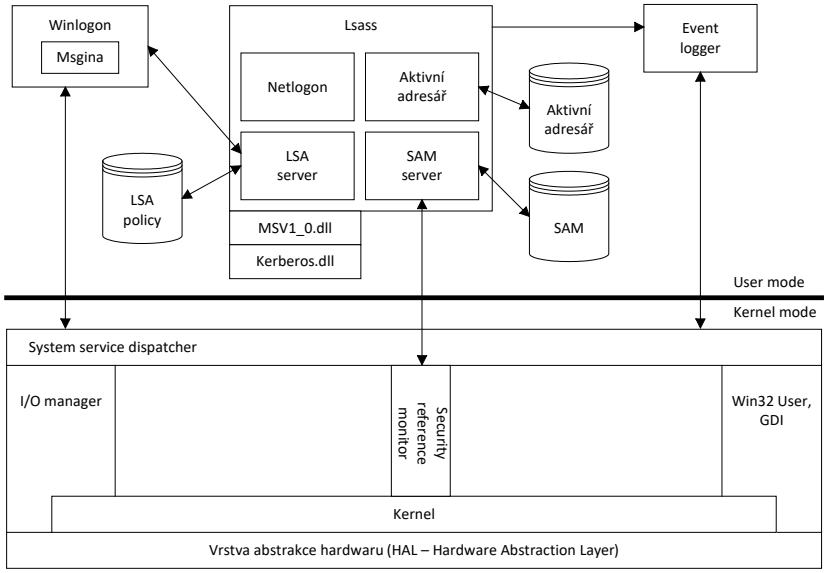
BEZPEČNOST WINDOWS

BEZPEČNOSTNÍ PODSYSTÉM



Security reference monitor (SRM)

Část exekutivy Windows (\Winnt\System32\Ntoskrnl.exe), která řídí přístup k objektům operačního systému, zpracovává uživatelská práva (user rights) a generuje zprávy auditu.

Podsystém Local security authority (Lsass)

Proces běžící v uživatelském režimu (\Winnt\System32\Lsass.exe), který zodpovídá za místní bezpečnostní politiku (patří sem např. možnost přihlásit se k počítači, politika účtů, privilegia uživatelských a skupinových účtů, nastavení parametrů auditu), autentizaci uživatelů a zasílání auditních zpráv do odpovídajících log souborů. Většinu těchto funkcí implementuje knihovna Lsasrv (\Winnt\System32\Lsasrv.dll).

Databáze politiky Lsass

Databáze obsahující nastavení místní bezpečnostní politiky. Je součástí registru (HKLM\SECURITY). Obsahuje informaci o důvěryhodných doménách, o tom, kdo se může přihlásit k systému a jak (interaktivně, ze sítě), o přiřazení uživatelských práv a nastavení auditu. Také jsou v ní uložená tzv. úspěšná kešovaná přihlášení, pokud ovšem nebylo zakázáno jejich ukládání.

Služba Security Accounts Manager (SAM)

Služba spravuje databázi obsahující lokální uživatelské a skupinové účty. Služba SAM je implementována jako knihovna \Winnt\System32\Samsrv.dll a běží v rámci procesu Lsass.

Databáze SAM

Databáze, která obsahuje definované lokální uživatelské a skupinové účty spolu s jejich hesly a dalšími atributy. Databáze je součástí registru (HKLM\SAM), na disku ji lze najít ve \winnt\system32\config.

Aktivní adresář (Active Directory, AD)

Adresářová služba využívající databázi, která obsahuje informace o objektech domény. Doména je skupina počítačů, která je administrována jako jeden celek prostřednictvím společně sdílených objektů. Typickým objektem aktivního adresáře je uživatel, počítač, skupina a organizační jednotka. Také informace o heslech a uživatelských právech je uložena

v aktivním adresáři, kde se spolu s ostatním objekty replikuje mezi speciálně vyčleněnými počítači – tzv. řadiči domény. Proces serveru aktivního adresáře je implementován ve \Winnt\System32\Ntdsa.dll a běží v rámci procesu Lsass.

Autentizační balíky

Jsou to DLL knihovny běžící v kontextu Lsass procesu, které implementují autentizační politiku Windows. Autentizační balík kontroluje, zda je v pořádku uživatelem zadané jméno a heslo, a pokud ano, poskytne procesu Lsass podrobnou informaci o uživateli.

Přihlašovací proces (Winlogon)

Proces běžící v uživatelském režimu (\Winnt\System32\Winlogon.exe), který odpovídá na stisk kláves CTRL+ALT+DEL (jedná se o tzv. SAS, Security Attention Sequence) a řídí interaktivní přihlašování. Winlogon také po úspěšném přihlášení vytváří proces reprezentující uživatelské rozhraní (user shell, typicky se jedná o Explorer).

Grafická identifikace a autentizace (GINA)

DLL knihovna běžící v rámci procesu Winlogon, jejímž prostřednictvím Winlogon získá jméno účtu a heslo případně PIN čipové karty. Standardní GINA je \Winnt\System32\Msgina.dll.

Služba síťového přihlášení (Netlogon)

Služba (\Winnt\System32\Netlogon.dll), která běží uvnitř Lsass a odpovídá na přihlašovací požadavky ze sítě. Autentizace se pak provede podobně jako u interaktivního (lokálního) přihlášení. Služba Netlogon je také schopna lokalizovat řadiče v doméně.

Kernel Security Device Driver (KSecDD)

Knihovna funkcí implementujících LPC rozhraní (LPC – Local Procedure Call), které využívají ostatní bezpečnostní moduly běžící v režimu jádra. Například šifrovaný souborový systém (EFS – Encrypting File System) ji využívá pro komunikaci s Lsass. Ovladač KSecDD je obsažen ve \Winnt\System32\Drivers\Ksecdd.sys.

BEZPEČNOSTNÍ IDENTIFIKÁTORY (SID)

Ve Windows se uživatelé i některé další objekty (lokální a globální skupiny, počítače, domény) označují jedinečnými identifikátory (SID – Security Identifier). Vždy, když administrátor pracuje například se jménem uživatelského účtu, operační systém toto jméno zobrazil jako náhradu příslušného SIDu. SID je numerický řetězec s proměnnou délkou, který se skládá z několika částí:

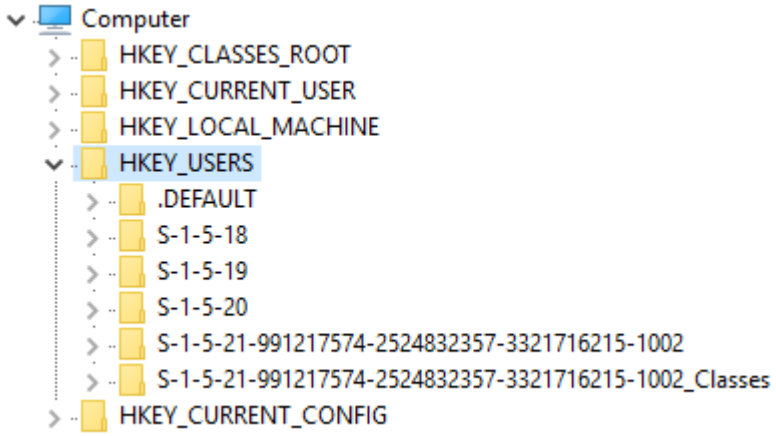
- označení autority a podautority, která SID vytvořila,
- 48-bitový identifikátor,
- relativní identifikátor (RID, např. účet Administrátor má RID = 500).

Pokud je SID někde v systému zobrazen, obsahuje navíc prefix S a jeho jednotlivé části jsou odděleny pomlčkou: S-1-5-21-1463437245-1224812800-863842198-1128. SIDy jsou dostatečně dlouhé a operační systém je generuje dostatečně náhodně, aby nedošlo k duplicitě ani na počítači ani v doméně.

Při instalaci Windows vytvoří setup SID počítače. Operační systém přiděluje SID každému lokálnímu účtu, přičemž tento SID je založen na SIDu počítače a na konci má specifický RID. RIDy pro uživatelské účty a skupiny začínají od hodnoty 1000 a zvětšují se o jedničku. Podobně má přiřazený jedinečný SID i nově vytvořená doména. Doménové účty pak mají SIDy založené na SIDu domény a na konci mají opět RIDy od 1000 výše. Například RID 1028 znamená, že jde o dvacátýdevátý SID, který doména přiřadila účtu.

Ne všechny SIDy jsou skutečně jedinečné. Existují tzv. dobře známé SIDy (well-known SIDs), které jsou naopak na všech počítačích stejné. Také standardní systémové účty a skupiny mají pevně přidělené RIDy (SID počítače je samozřejmě jedinečný). Tak například RID = 500 má účet Administrator, RID = 501 účet Guest.

S-1-1-0	Skupina Everyone.
S-1-3-0	Skupina Creator Owner, při dědění ACE nahradí operační systém tento SID SIDem uživatele, který objekt vytvořil.
S-1-5-2	Skupina Network obsahuje všechny uživatele přihlášené ze sítě.
S-1-5-4	Skupina Interactive obsahuje všechny uživatele přihlášené lokálně pomocí klávesnice.
S-1-5-18	Účet System reprezentující operační systém.
S-1-5-19	Účet Local Service.
S-1-5-20	Účet Network Service.
S-1-5-domain-500	Účet Administrator.
S-1-5-domain-501	Účet Guest nevyžaduje zadání hesla. Standardně je vypnut.
S-1-5-32-544	Zabudovaná lokální skupina Administrators. Zpočátku je jejím jediným členem účet Administrator. Po přidání počítače do domény se členem stane i globální skupina Domain Admins. Pokud se server stane řadičem domény, přidá se do skupiny Administrators i globální skupina Enterprise Admins.
S-1-5-32-545	Zabudovaná lokální skupina Users.
S-1-5-32-546	Zabudovaná lokální skupina Guests.



Se SIDy se lze setkat například v registru, po spuštění editoru registru (regedit.exe). V části HKEY_USERS jsou uložena data specifická pro přihlášené uživatele.

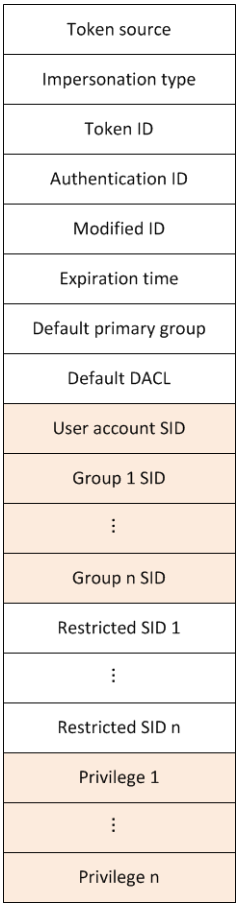
Z příkazové řádky lze SIDy zjistit například takto:

```
whoami /all
wmic useraccount list brief
wmic group
```

Přístupová známka (Access Token)

Modul SRM používá k identifikaci bezpečnostního kontextu procesu zvláštní datovou strukturu zvanou přístupová známka (access token). Bezpečnostní kontext je tvořen informací o privilegiích, uživatelských účtech a skupinách, které jsou s procesem spojeny. Přístupová známka je vytvořena na konci přihlašovacího procesu. V okamžiku, kdy dojde k ověření jména a hesla, je Winlogon schopen potřebnou informaci získat ze SAM databáze, z databáze politiky Lsass, případně z aktivního adresáře, podle toho, zda se uživatel hlásí prostřednictvím lokálního nebo doménového účtu.

Winlogon vytvoří přístupovou známku a spustí Explorer, kterému ji předá. Všechny programy, které uživatel spustí, obdrží svou kopii přístupové známky. Další kopie lze vytvořit voláním funkce Win32 rozhraní LogonUser. Přístupová známka má různou délku, protože uživatelé se ve svých privilegiích i členstvím ve skupinách liší. Následující obrázek charakterizuje informace, které přístupová známka obsahuje.



Bezpečnostní mechanismus Windows využívá jednotlivé části přístupové známky k tomu, aby určil, zda může proces získat přístup k některému ze zabezpečených objektů, jako například k souboru na NTFS disku. Konkrétně se jedná o pole SID uživatelova účtu a SIDy skupin, jejichž je uživatel členem.

Také pole privilegií určuje, co může proces v systému provádět. Pole privilegií představuje seznam práv spojených s přístupovou známkou. Příkladem privilegia může být právo vypnout počítač, nastavit systémový čas apod. Těchto privilegií je kolem dvaceti a některá z nich uvádí následující tabulka.

Privilegium	Význam
SeBackup	Obchází kontrolu přístupových práv při zálohování.
SeDebug	Používá se při ladění procesu.
SeShutdown	Umožňuje vypnout počítač.
SeTakeOwnership	Umožňuje převzít vlastnictví objektu a to i v případě, že k němu jinak nemá přístup. Po převzetí vlastnictví objektu lze modifikovat seznam přístupových práv.

Pole Default primary group a Default DACL využívá proces při vytváření nových objektů. Obsahují bezpečnostní atributy, které budou nově vytvořenému objektu předány.

Přístupové známky lze rozdělit na primární a zosobňovací. Primární přístupová známka určuje bezpečnostní kontext procesu. Zosobňovací přístupová známka je procesem použita, když potřebuje dočasně převzít bezpečnostní kontext jiného uživatele.

BEZPEČNOSTNÍ DESKRIPTORY A ŘÍZENÍ PŘÍSTUPU

Další důležitou datovou strukturou jsou bezpečnostní deskriptory, které jsou spojeny s objekty operačního systému jako je soubor, adresář, tiskárna, sdílený adresář, položka registru a objekt v aktivním adresáři. Bezpečnostní deskriptor obsahuje následující informace:

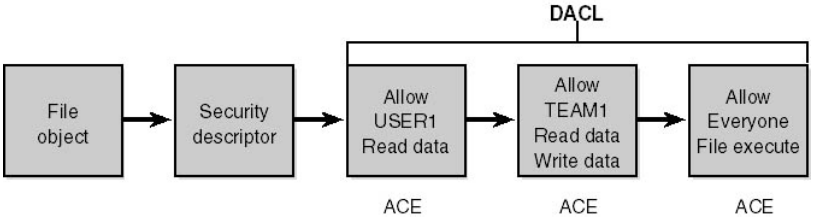
- Číslo verze.
- Příznaky – volitelné parametry modifikující vlastnosti deskriptoru. Například příznak SE_DACL_PROTECTED zabrání deskriptoru v dědění bezpečnostního nastavení z nadřízeného objektu.
- SID vlastníka.
- SID skupiny identifikující tzv. primární skupinu objektu (využito jen v POSIXu).
- DACL (Discretionary access-control list) určuje, kdo bude mít přístup k objektu.
- SACL (System access-control list) určuje, jaké operace a jakých uživatelů budou zaznamenány do bezpečnostního logu (viz audit).

Seznam přístupových práv (ACL – Access Control List) obsahuje záhlaví a několik položek pro řízení přístupu (ACE – Acces Control Entry). Rozlišují se dva typy ACL: DACL a SACL. DACL má ACE položky obsahující SID a přístupovou masku, které mohou být čtyř typů: access allowed, access denied, allowed-object a denied-object. První typ – podle očekávání – zaručuje uživateli přístup k objektu, druhý typ mu přístup k objektu zakazuje. Třetí a čtvrtý typ se chová podobně jako první a druhý, ale používá se jen v aktivním adresáři, přičemž objekty, se kterými je spojen, identifikuje pomocí globálně jedinečných identifikátorů (GUID).

Přístupové právo uživatele k objektu vzniká složením všech ACE položek v seznamu DACL. Pokud v deskriptoru DACL není, bude mít k objektu úplný přístup každý (člen skupiny Everyone). Pokud tam DACL je, ale neobsahuje žádnou ACE položku, nebude moci k objektu přistupovat nikdo.

Jednotlivé ACE položky v DACL seznamu mohou mít také příznaky, které souvisí s děděním přístupových práv, protože některé objekty mohou obsahovat další objekty a ty zase další atd. (například adresáře, podadresáře a soubory nebo klíče registru).

Seznam SACL obsahuje jen dva typy ACE položek: system audit a system audit-object. Pomocí těchto položek lze určit, které operace s objektem a pro které uživatele se mají zaznamenat do auditu, konkrétně do tzv. bezpečnostního log souboru. Zaznamenávat se mohou operace úspěšné i neúspěšné. Příznaky dědičnosti v případě SACL fungují stejně jako v případě seznamu DACL.



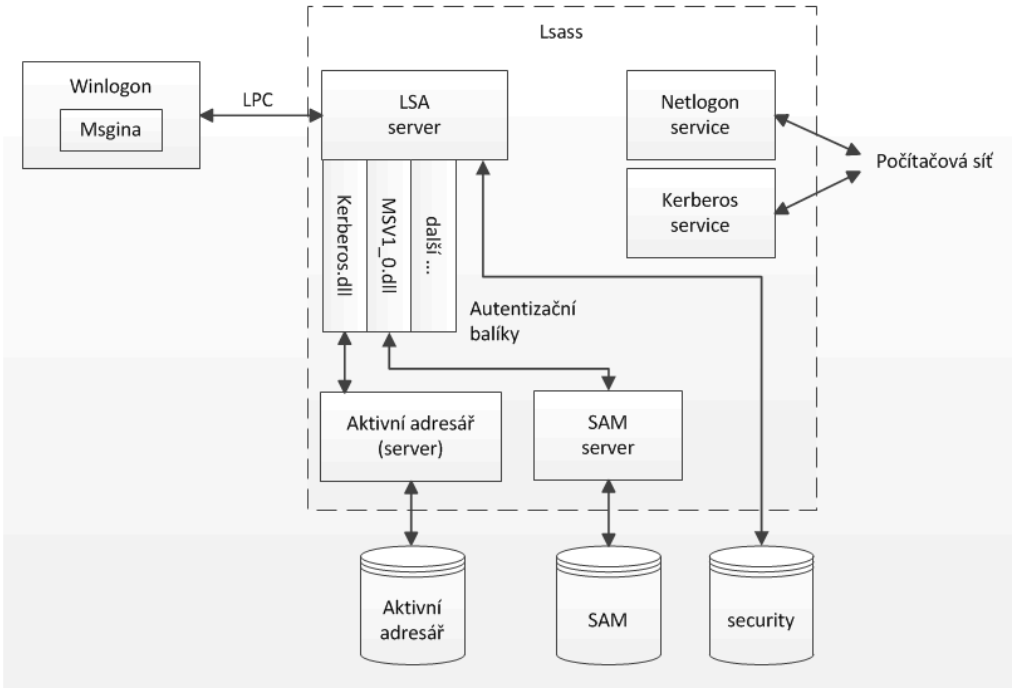
PŘIHLÁŠENÍ

Interaktivní přihlášení probíhá ve spolupráci přihlašovacího procesu Winlogon, modulu Lsass, jednoho či více autentizačních balíků a SAM nebo aktivního adresáře. Autentizační balík je DLL knihovna, která provádí autentizaci uživatele. Například Kerberos je autentizační balík pro interaktivní přihlášení k doménovému účtu, zatímco balík MSV1_0 se používá při přihlášení k lokálnímu účtu nebo když je řadič domény nedostupný.

Winlogon je proces, který přihlašování koordinuje. Kromě toho ale také na závěr úspěšného přihlášení spouští Explorer, zařizuje odhlášení uživatele, umožňuje zadat přihlašovací heslo, změnit heslo, zamknout a odemknout počítač. Proces Winlogon musí zajistit, že tyto operace, které souvisí s bezpečností, nebudou „viditelné“ pro ostatní aktivní procesy.

Winlogon získá jméno uživatele a jeho heslo prostřednictvím DLL knihovny zvané GINA (Graphical Identification and Authentication). Standardní knihovnou je Msgina (\Winnt\System32\ Msgina.dll), která zobrazuje přihlašovací okno Windows. Pokud dojde k jejímu nahrazení jinou DLL knihovnou, lze k identifikaci uživatele použít i jiný způsob, než je jméno účtu a heslo. Může jít například o nějaké biometrické zařízení.

Jedině Winlogon zachytí přihlašování prostřednictvím klávesnice. Poté, co obdrží jméno a heslo od GINy, požádá Lsass o autentizaci uživatele. Spolupráce těchto komponent je zachycena na následujícím obrázku.



Během inicializace operačního systému, ještě předtím, než se spustí libovolná aplikace, provede Winlogon několik operací. Vytvoří a otevře interaktivní stanici \Windows\WinSta0, která reprezentuje klávesnici, myš a monitor. Vytvoří pro ní bezpečnostní deskriptor, který obsahuje jedinou ACE položku se SIDem procesu Winlogon. Tím zajistí, že se bez jeho povolení k počítači nedostane žádný jiný proces. Dále vytvoří tři desktopy (pracovní plochy): aplikační desktop (\Windows\WinSta0\ Default), Winlogon desktop (\Windows\WinSta0\Winlogon) a desktop spořiče obrazovky (\Windows\WinSta0\Screen-Saver). Winlogon desktop je přístupný jen procesu Winlogon, ostatní mohou využívat i uživatelé. Tak je zajištěno, že je-li aktivní Winlogon desktop, žádný jiný proces nemá přístup ke kódu nebo datům s tímto desktopem spojeným. Tak je chráněna například změna hesla uživatele nebo zamykání či odemykání počítače.

PROCES PŘIHLÁŠENÍ UŽIVATELE

Přihlášení začíná v okamžiku, kdy uživatel stiskne SAS sekvenci – kombinaci kláves Ctrl+Alt+Delete. Poté Winlogon zavolá GINu a obdrží jméno a heslo. Dále zavolá registrované autentizační balíky, které jsou uvedeny v registru (HKLM\SYSTEM\CurrentControlSet\Control\Lsa). Typicky se jedná o balík MSV1_0 nebo Kerberos.

MSV1_0 převezme jméno uživatele a hash hodnotu hesla a požádá modul SAM o informace s tímto účtem spojené (skupiny, jejichž je členem, a různá omezení účtu). MSV1_0 kontroluje omezení účtu, například dobu, kdy je možné účet k přihlášení použít. Pokud se uživatel nemůže kvůli těmto omezením přihlásit, ohlásí MSV1_0 chybu modulu LSA. V opačném případě porovná jméno uživatele a hash hodnotu hesla s informací uloženou v SAM databázi. Pokud to systém povoluje, může místo toho využít některé z kešovaných přihlášení, které najde v LSA databázi (v registru jde o klíč SECURITY).

Jestliže data zadaná uživatelem odpovídají těm v databázi, vygeneruje MSV1_0 identifikátor LUID (Locally Unique Identifier) pro přihlašovací sezení, které vzápětí spustí.

K autentizaci může dojít i na vzdáleném počítači, jako je tomu v případě, že se uživatel přihlásil prostřednictvím účtu z domény Windows NT 4.0. V takovém případě spolupracuje MSV1_0 s lokální službou NetLogon. Ta komunikuje se vzdálenou službou Netlogon a ta zase se vzdáleným autentizačním balíkem MSV1_0. Výsledek autentizace služby NetLogon přenesou zpět na lokální počítač.

Kerberos autentizace je v principu schodná s autentizací realizovanou balíkem MSV1_0. Tentokrát je však mnohem pravděpodobnější, že při autentizaci bude potřeba přenášet data po síti (komunikuje se totiž s řadičem). Balík Kerberos k tomu využívá Kerberos TCP/IP port (port 88) a službu Kerberos, která běží na řadiči domény. Služba Kerberos (\Winnt\System32\Kdcsvc.dll) implementuje protokol Kerberos verze 5.

K ověření jména a hash hodnoty hesla použije server aktivního adresáře (\Winnt\System32\ Ntdsa.dll) informaci z databáze a v případě úspěchu je vše potřebné předáno zpět modulu Lsass.

Po úspěšné autentizaci řízení přebírá Lsass. Nejprve zjistí, zda má uživatel povolen ten způsob přihlášení, který zvolil. Pokud zvolil uživatel interaktivní přihlášení a má ho povoleno (právo Log on locally), přidá Lsass k informaci, kterou zatím získal, další příslušné SIDy (pro skupiny Everyone, Interactive nebo Network) a privilegia. Pokud uživatel zvolený způsob přihlášení povolen nemá, Lsass zruší přihlašovací sezení, vymaže všechny s ním svázané datové struktury a ohlásí chybu procesu Winlogon.

Nyní má Lsass věškerou potřebnou informaci a proto požádá exekutivu Windows o vytvoření přístupové známky. Exekutiva vytvoří primární přístupovou známku pro interaktivní přihlášení nebo zosobňovací přístupovou známku pro síťové přihlášení. Lsass známku předá procesu Winlogon.

Winlogon se podívá do registru na hodnotu klíče HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\Userinit a vytvoří proces pro spuštění obsahu tohoto klíče (typicky jde o několik exe souborů, oddělených čárkou). Standardně klíč obsahuje řetězec Userinit.exe. Jde o program, který načte uživatelský profil a spustí program, jehož jméno je uvedeno v klíči registru HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\Shell. Tento klíč standardně obsahuje program Explorer.exe.

BEZPEČNOST SOUBORŮ A ADRESÁŘŮ

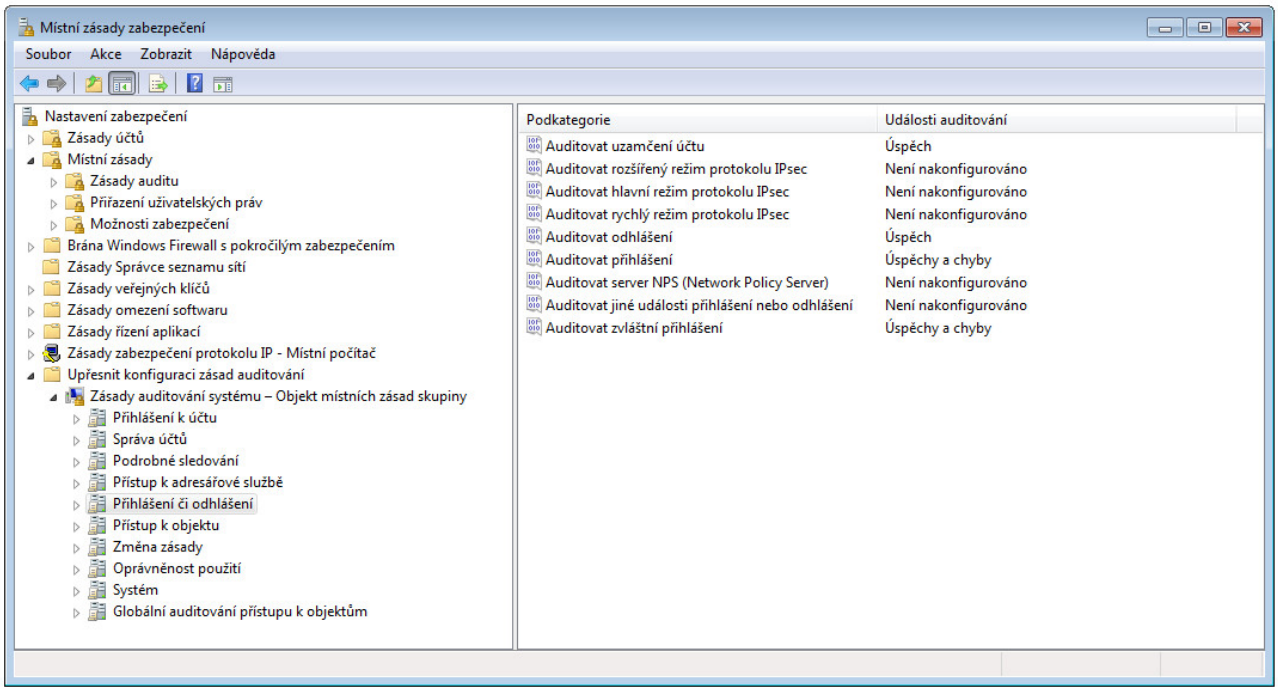
- Bezpečnost je zajištěna přístupovými právy definovanými v bezpečnostním deskriptoru. Jedná se o lokální bezpečnost na NTFS disku, nebo o síťovou bezpečnost, pokud uživatel k souboru přistupuje prostřednictvím sdíleného adresáře.
- Nový soubor dědí přístupová práva adresáře v němž se nachází.
- Přístupová práva se sčítají, s výjimkou přístupového práva „Deny“, které všechno převáží.
- Při kopírování v rámci jednoho oddílu disku (partition) zdědí soubor či adresář přístupová práva cílového adresáře.
- Při přesunu mezi různými oddíly zdědí soubor či adresář přístupová práva cílového adresáře. Při přesunu v rámci jednoho oddílu si soubor zachová původní přístupová práva.
- Při přesunu z NTFS disku na FAT disk se přístupová práva ztrácejí, protože FAT nemá bezpečnostní deskriptory.

SDÍLENÉ PROSTŘEDKY

- Sdílet adresáře mohou pouze členové skupiny Administrators a Power Users.
- Pro potřeby administrace systému vytváří Windows zvláštní sdílené adresáře (Admin$, Print$, C$, D$ atd.), ke kterým mají přístup jen administrátoři. Tyto sdílené adresáře končí znakem dolar ($), takže pro normální uživatele jsou neviditelné.
- Sdílená přístupová práva (definovaná v bezpečnostním deskriptoru sdíleného adresáře) se aplikují jen tehdy, pokud se k adresáři přistupuje ze sítě. Standardní sdílené přístupové právo je Full Control pro skupinu Everyone. Sdílená přístupová práva platí nejen pro NTFS, ale i pro souborové systémy FAT a FAT32.

AUDIT

Události související s bezpečností operačního systému se zaznamenávají do bezpečnostního logu. Kromě něj existuje ještě aplikační log, do kterého zaznamenávají události některé ze spuštěných aplikací, a systémový log, který využívá samotný operační systém - například k zápisu informací o průběhu svého spouštění, zavádění ovladačů a spouštění služeb. Další logy se vytvářejí v závislosti na roli, jakou počítač v síti plní. Vlastní logy tak má adresářová služba, DNS server a služba replikace souborů. Prohlížet obsah log souborů a konfigurovat jejich vlastnosti umožňuje nástroj Event Viewer.



Audit se konfiguruje v nástroji administrátora Místní zásady zabezpečení (secpol.msc).

Poznámka: V nástroji Místní zásady zabezpečení lze audit konfigurovat dvěma různými způsoby, které se nemají navzájem kombinovat. Přes Místní zásady → Zásady auditu, může administrátor konfigurovat 9 kategorií událostí, přes Upřesnit konfiguraci zásad auditování → Zásady auditování systému pak 10 kategorií, které se dále dělí asi do 50 podkategorií. První způsob byl typický pro Windows XP, druhý způsob se používá u Windows 7 a novějších verzí Windows.

Pokud chceme sledovat přístup k objektům, jako jsou soubory, adresáře, tiskárny a klíče registru, musí být nejprve povolena politika Audit object access. To ale nestačí, ještě je třeba upravit SACL (System Acces Control List). Například u adresáře a souboru stačí kliknout pravým tlačítkem myši a zvolit Vlastnosti → panel Zabezpečení → tlačítko Upřesnit → panel Auditování. Soubory a adresáře lze sledovat jen tehdy, pokud se nachází na NTFS disku, protože FAT disky audit nepodporují. Audit tiskárny se nastavuje podobně jako u souboru či adresáře, audit klíčů registru se nastavuje pomocí nástroje pro editaci registru regedit.exe. Úpravu SACL typicky provádí administrátor, přičemž určí uživatele a skupiny, jejichž přístup k objektu chce sledovat; spolu s typem přístupu, který ho zajímá.

Pro Windows XP a bezpečnostní log jsou typické identifikátory událostí od 528 do 539.

Id události	Význam
528	Úspěšné přihlášení
529	Neúspěšné přihlášení - neznámé jméno uživatele nebo špatné heslo
530	Neúspěšné přihlášení - v uvedenou dobu je zakázáno přihlášení
531	Neúspěšné přihlášení - účet je zakázán (disabled)
532	Neúspěšné přihlášení - platnost účtu již vypršela
533	Neúspěšné přihlášení - uživatel nemá povoleno místní přihlášení

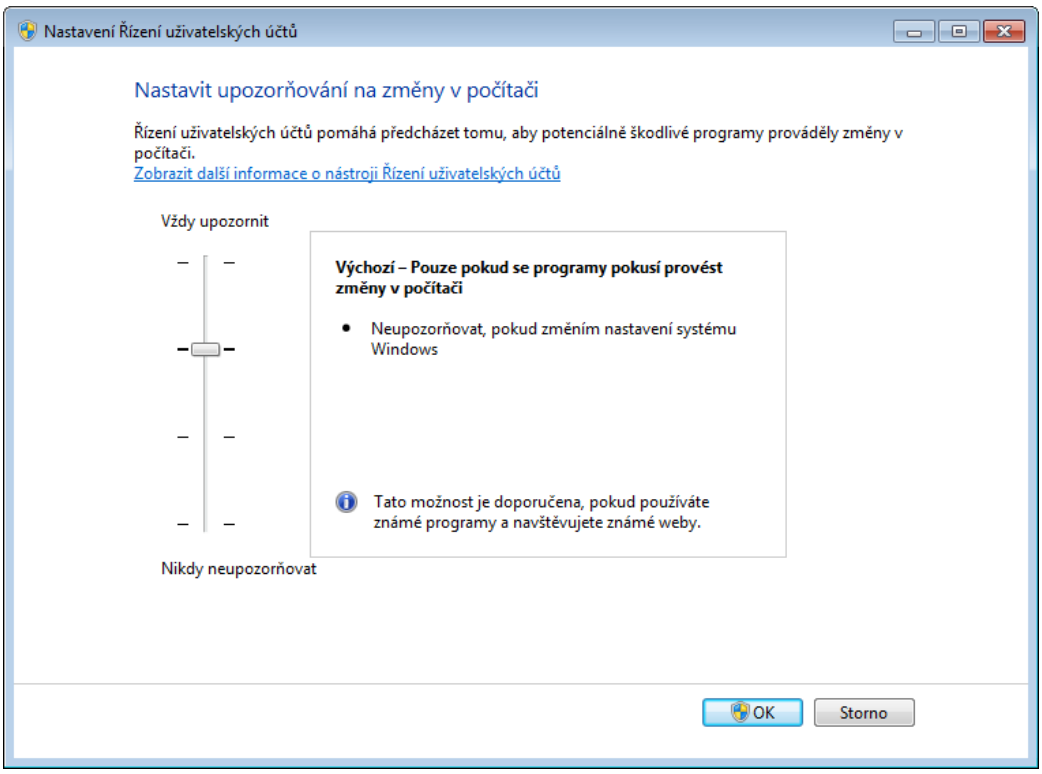
534	Neúspěšné přihlášení - požadovaný typ přihlášení nemá uživatel povolen Typy přihlášení: 2 - místní (interactive) z klávesnice, 3 - síťové, např. ke sdílenému adresáři, 4 - dávkový soubor, 5 – služba, 7 - odemčení heslem chráněného spořiče obrazovky
535	Neúspěšné přihlášení - vypršela platnost hesla k tomuto účtu
539	Neúspěšné přihlášení - účet je uzamčen

Ve Windows 7 se administrátor zaměřuje na jiné identifikátory událostí

Id události	Význam
4624	Úspěšné přihlášení (Auditovat přihlášení)
4625	Neúspěšné přihlášení (Auditovat přihlášení) (chybový kód události upřesňuje důvod neúspěchu)
4647	Uživatel se odhlásil (Auditovat odhlášení)
4688	Vytvoření procesu
4689	Ukončení procesu
4616	Změna času
4800	Uzamknutí pracovní plochy (Auditovat jiné události přihlášení nebo odhlášení)
4801	Odemknutí pracovní plochy (Auditovat jiné události přihlášení nebo odhlášení)
4802	Vyvolán šetřič obrazovky
4720	Vytvoření účtu (Auditovat správu účtů uživatelů)
4724	Reset hesla (Auditovat správu účtů uživatelů)
4725	Účet byl zakázán (Auditovat správu účtů uživatelů)
4726	Smazání účtu (Auditovat správu účtů uživatelů)
4732	Přidání do skupiny (Auditovat správu účtů uživatelů)
4738	Změna účtu (Auditovat správu účtů uživatelů)
4740	Uzamknutí účtu (Auditovat správu účtů uživatelů)
4767	Odemknutí účtu (Auditovat správu účtů uživatelů)

NASTAVENÍ NÁSTROJE ŘÍZENÍ UŽIVATELSKÝCH ÚČTŮ

Nástroj Řízení uživatelských účtů (UAC) vás upozorní před provedením změn v počítači, které vyžadují oprávnění správce. Výchozí nastavení Řízení uživatelských účtů (UAC) vás upozorní, než se programy pokusí o provedení změn v počítači, ale máte možnost změnit četnost tohoto upozorňování.



Následující seznam poskytuje popis nastavení Řízení uživatelských účtů (UAC) a možný dopad jednotlivých nastavení na zabezpečení vašeho počítače.

Vždy upozornit

Zobrazí se upozornění, než programy provedou změny vašeho počítače nebo nastavení systému Windows, které vyžaduje oprávnění správce.

Při zobrazení upozornění se ztmaví plocha a musíte schválit nebo zamítnout požadavek v dialogovém okně nástroje Řízení uživatelských účtů předtím, než budete moci dále pracovat s počítačem. Ztmavení plochy se označuje jako zabezpečená plocha, protože ve chvíli, kdy je aktivní, nelze spouštět jiné programy. Toto nastavení poskytuje nejvyšší úroveň zabezpečení. Po upozornění byste si měli pečlivě přečíst obsah každého dialogového okna, než povolíte provedení změn v počítači.

Upozorňovat pouze v případě, pokud se programy pokusí provést změny v počítači

Zobrazí se upozornění, než programy provedou změny vašeho počítače nebo nastavení, které vyžaduje oprávnění správce. Pokud se při pokusíte o provedení změn v nastavení systému Windows, které vyžaduje oprávnění správce, upozornění se nezobrazí.

Upozornění se zobrazí, pokud se program mimo systém Windows pokusí provést změny nastavení systému Windows. Obvykle je bezpečné povolit provádění změn nastavení systému Windows bez upozorňování. Některé programy dodané se systémem Windows však mohou obsahovat příkazy a data, která jsou do nich předávána, a škodlivý software toho může využít zneužitím těchto programů k instalaci souborů nebo provedení změn nastavení počítače. Vždy byste měli opatrně zvážit, které programy povolíte v počítači spouštět.

Upozorňovat pouze v případě, pokud se programy pokusí provést změny v počítači (nestmívat plochu)

Zobrazí se upozornění, než programy provedou změny vašeho počítače nebo nastavení, které vyžaduje oprávnění správce. Pokud se při pokusíte o provedení změn v nastavení systému Windows, které vyžaduje oprávnění správce, upozornění se nezobrazí.

Upozornění se zobrazí, pokud se program mimo systém Windows pokusí provést změny nastavení systému Windows. Toto nastavení je stejné jako nastavení v okně Pouze pokud se programy pokusí provést změny v počítači, ale nebudete upozornění na zabezpečené ploše.

Nikdy neupozorňovat

Nebudete upozornění před provedením změn v počítači. Pokud jste přihlášení jako správce, mohou programy provádět změny v počítači bez vašeho vědomí. Pokud jste přihlášení jako standardní uživatel, budou jakékoli změny vyžadující oprávnění správce automaticky zamítnuty.

Jestliže vyberete toto nastavení, bude nutné proces vypnutí Řízení uživatelských účtů dokončit restartováním počítače. Jakmile bude nástroj Řízení uživatelských účtů vypnut, uživatelé, kteří se přihlašují pomocí účtu správce, budou mít vždy oprávnění správce. Toto nastavení poskytuje nejnižší úroveň zabezpečení. Pokud zakážete upozorňování nástroje Řízení uživatelských účtů, vystavujete počítač potenciálním bezpečnostním rizikům.

Jestliže program Řízení uživatelských účtů nastavíte tak, abyste nebyli nikdy upozorňováni, měli byste si dávat pozor, které programy spouštíte, protože budou mít stejný přístup k počítači jako vy. Patří sem čtení a provádění změn chráněných systémových oblastí, vašich osobních údajů, uložených souborů a jakýchkoli dalších položek uložených v počítači. Programy budou také mít povoleno komunikovat a přenášet informace mezi vzdálenými počítači a místním počítačem, a to včetně sítě Internet.

AUTENTIZAČNÍ PROTOKOLY WINDOWS

Autentizace je proces ověřující identitu uživatele. Aby měl operační systém jistotu, že uživatel je opravdu tím kým tvrdí, že je, požaduje po uživateli nějaký důkaz. Pro tento důkaz se v literatuře používá označení uživatelské pověření (user credentials), dále jen pověření. Pověření reprezentuje nějaký typický znak nebo jedinečnou informaci, která je v okamžiku autentizace dostupná všem zúčastněným stranám. Pověření se obvykle dělí do tří tříd. Může to být:

Něco, co známe. Tajemství, které známe a sdílíme ho se systémem, ke kterému chceme získat přístup, představuje nejjednodušší a nejobvyklejší formu pověření. Typickým příkladem je heslo.

Něco, co máme. Druhá třída pověření předpokládá, že uživatel vlastní nějaký autentizační předmět, například čipovou kartu, nějaké USB zařízení nebo RSA SecurID zařízení generující hesla na jedno použití.

Něco, co jsme. Třetí třída pověření zahrnuje širokou škálu biometrických informací jako jsou otisky prstů, oční duhovka, charakteristika hlasu, atd.

Autentizace může být jednofaktorová nebo vícefaktorová, podle toho, kolik různých typů pověření se při ní použije.

UKLÁDÁNÍ POVĚŘENÍ

Pověření použitá uživateli při autentizaci si operační systém musí někam ukládat. Hesla se standardně v otevřeném tvaru nikam neukládají, místo toho se ukládají jejich hash hodnoty. Hash hodnoty hesel k lokálním uživatelským účtům jsou uloženy přímo v počítači, kde byly účty založeny, v tzv. SAM databázi. Doménové účty se nacházejí v aktivním adresáři počítače, který vykonává funkci řadiče domény, a v jednom z atributů doménového účtu je uložena hash hodnota hesla.

Pro zvýšení bezpečnosti uložení hash hodnot používají některé systémy tzv. solení hesel, ale Windows k nim bohužel nepatří. To znamená, že dva uživatelé, kteří si náhodou zvolí stejné heslo, budou mít i stejnou hash.

Z důvodů zpětné kompatibility s operačním systémem LAN Manager jsou již od roku 1993 ve Windows řady NT podporovány méně bezpečné LM hashe. LAN Manager povoloval maximálně heslo dlouhé 14 znaků a v něm, kromě číslic a dalších povolených znaků jen velké znaky anglické abecedy. Postup při vytváření LM hashe je následující:

1. všechny znaky hesla se převedou na velké znaky,
2. heslo se dále doplní nulami na 14 znaků,
3. těchto 14 znaků se rozdělí na dvě skupiny po sedmi znacích,
4. každá skupina se použije jako klíč v algoritmu DES k zašifrování konstanty AAD3B435B51404EE,
5. zřetězením vznikne hash hodnota dlouhá 32 znaků.

Problém je, že pokud by se útočník dostal k těmto hash hodnotám, velmi rychle z nich získá původní hesla. Proto se v praxi generování LM hashe vypíná a používá se jen bezpečnější NT hash, která vzniká jako výstup z algoritmu MD4.

Pro testování útoků na LM hash je naopak možné povolit generování LM hashí pomocí postupu: secpol.msc → Místní zásady → Možnosti zabezpečení → Zabezpečení sítě: Neukládat hodnotu hash programu LAN Manager při příští změně hesla → Zakázáno.

Ve Windows XP je generování LM hashí standardně povoleno, ve Windows 7 zakázáno.

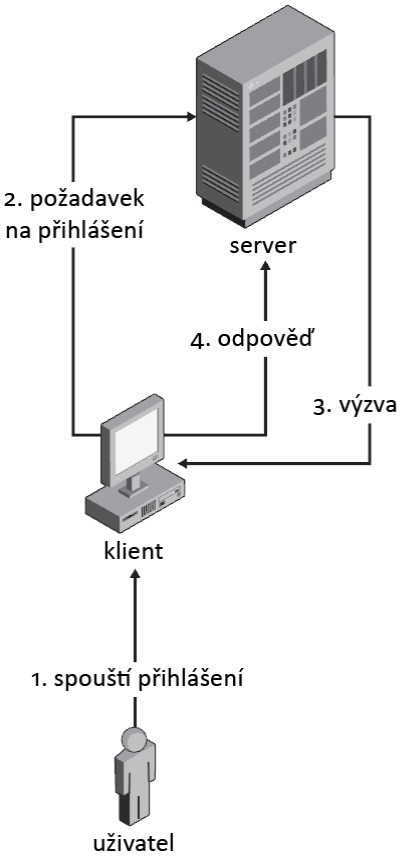
Pokud se uživatel úspěšně přihlásí do systému Windows pomocí doménového účtu, tak se standardně vytvoří lokální kopie hash hodnoty hesla, která mu později umožní se opakovaně přihlásit i v případě, že řadič domény nebude k dispozici. Toto "kešované pověření" je ale uloženo bezpečněji, protože standardní NT hash hodnota se spolu se jménem účtu (toto je jediný případ, kdy Windows použijí solení hesel) znovu zpracuje algoritmem MD4. Windows Vista a vyšší navíc přidávají ještě jeden krok: výsledná hodnota se zpracuje ještě algoritmem PKCS#5.

Přihlášení k lokálnímu účtu

Nejjednodušší varianta autentizace nastává v situaci, kdy se uživatel přihlašuje interaktivně na lokální účet. Uživatel stiskne kombinaci kláves Ctrl + Alt + Delete, načež část bezpečnostního podsystému Windows nazvaná LSASS (Local Security Authority Sub-System) vytvoří novou relaci a spustí proces WinLogon, který zobrazí přihlašovací dialogové okno.

Uživatel zadá jméno účtu a heslo. Proces WinLogon z hesla vytvoří NT hash, kterou porovná s hodnotou v SAM databázi. Jsou-li obě hodnoty stejné, je přihlášení úspěšně dokončeno.

Pokud se ovšem hlásíme přes síť k vzdálenému počítači nebo pomocí doménového účtu, situace se komplikuje, protože se musíme strachovat o to, v jakém tvaru putuje autentizační informace po síti. Ve Windows v takovém případě vzniká mnoho různých scénářů, které však mají společné to, že se v nich využívá nějaká varianta protokolu typu výzva – odpověď. Obecné schéma protokolu zachycuje následující obrázek.



Obecné schéma protokolu typu výzva – odpověď.

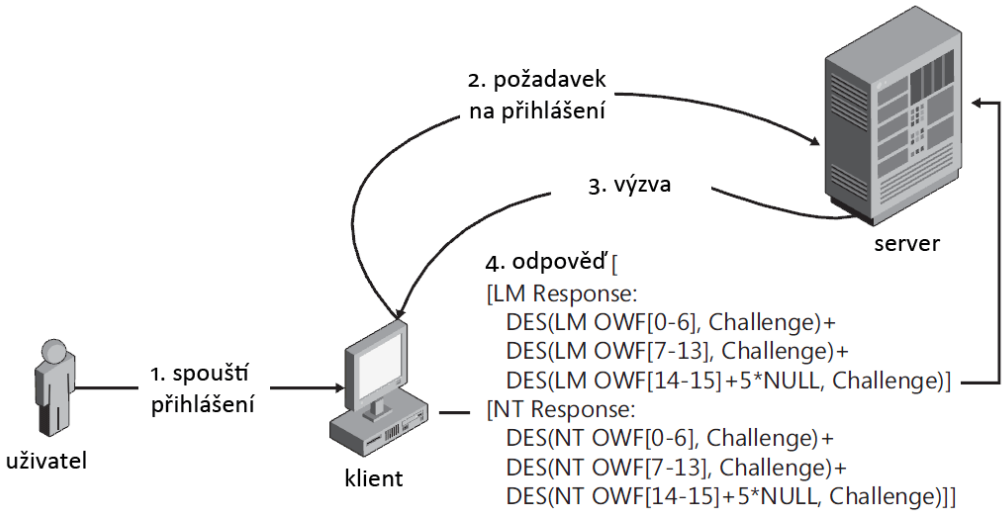
Uživatel zahájí přihlašování tím, že vznese požadavek na vzdálený server. Server vytvoří tzv. výzvu, což je nějaká náhodná hodnota, kterou pošle klientovi. Klient má k dispozici informaci, kterou uživatel zadal při lokálním příhlášení, a tuto informaci zpracuje spolu s výzvou v kryptografické operaci jejímž výstupem je odpověď serveru.

NTLM a Kerberos jsou jsou dva standardní protokoly Windows odpovídající výše popsanému schématu.

PROTOKOL NTLM

NTLM označuje rodinu autentizačních protokolů, která byla postupně vylepšována v závislosti na tom, jaké bezpečnostní hrozby se objevovaly. Všechny verze Windows řady NT až do Windows Server 2003, posílaly současně LM odpověď i NT odpověď. Žádná domluva o tom, která z variant prokolu se použije neprobíhala.

Od verze Windows Server 2003 je standardně zasílána jen NT odpověď, Windows Vista a vyšší upřednostňují bezpečnější variantu protokolu označovanou jako NTLM v2. Starší verze Windows mohou NTLM v2 používat také, ale musí být tak nakonfigurovány, nejedná se tedy o standardní chování. Konfigurovatelná položka registru se v originále nazývá LMCompatibilityLevel, ale administrátor ji typicky nemodifikuje přímo v registru, místo toho používá nástroj **Místní zásady zabezpečení** nebo modifikuje GPO objekt v aktivním adresáři. (V češtině se položka nazývá **Zabezpečení sítě**: **Úroveň ověřování pro systém LAN Manager**.)



Starší verze Windows posílaly současně oba typy odpovědí.

Vylepšení NTLM v2 používá původní NT hash, kterou doplňuje výzva od klienta a v odpovědi se používá algoritmus HMAC-MD5. Odpověď obsahuje také časovou známku, která má zabránit útokům typu opakování zprávy.

Protokol Kerberos

Protokol Kerberos je preferovaným autentizačním protokolem v doméně od verze Windows 2000. Pouze v situaci, kdy nelze použít, přejde se na některou z variant protokolu NTLM. Protože využívá tzv. plně kvalifikovaná doménová jména, nelze ho použít například tehdy, když chce uživatel využívat prostředky vzdáleného počítače identifikovaného jen IP adresou.

Kerberos umožňuje na rozdíl od NTLM vzájemnou autentizaci klienta i serveru. Protokol Kerberos také předpokládá, že síť představuje nepřátelské prostředí ve kterém může útočník odposlouchávat síťový provoz, zachycovat, mazat a modifikovat autentizační zprávy. Aby dosáhl bezpečné autentizace používá Kerberos nejen šifrování dat, ale také časovou synchronizaci. Kerberos ve verzi 5, který je implementován ve Windows, standardně předpokládá, že čas na klientovi a na serveru se neliší o více než pět minut.

Tok požadavků a odpovědí protokolu Kerberos ilustruje obrázek.

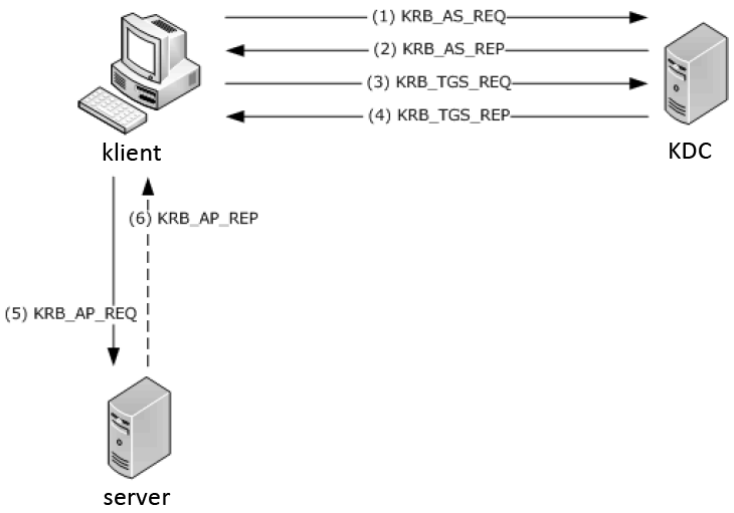
Po spuštění počítače jsou vytvořena tzv. předautentizační data, obsahující mimo jiné i časovou známku. Předautentizační data jsou zašifrována klíčem odvozeným z hesla a zaslána jako KRB_AS_REQ paket (Kerberos Authentication Service Request) autentizační službě, která se ve Windows označuje jako KDC (Key Distribuiton Center) a běží na řadiči domény.

Autentizační služba vytvoří speciální datovou strukturu označovanou jako TGT lístek (Ticket Granting Ticket). Dále vytvoří klíč relace, který klient použije při komunikaci s další službou běžící na řadiči domény – TGS (Ticket Granting Service, služba poskytující lístky). Tento klíč je klientovi zaslán šifrovaně jako KRB_AS_REP paket.

Klient nyní pošle požadavek službě poskytující lístky s žádostí o přístup ke vzdálenému serveru. Tento požadavek obsahuje TGT lístek, identifikaci služby na serveru a další informace, to vše šifrované klíčem relace.

Služba poskytující lístky odpoví zprávou obsahující lístek pro požadovanou službu, který obsahuje mimo jiné informaci získanou od klienta v předchozím kroku. Celé je to zašifrované veřejným klíčem serveru, takže pro klienta je to nečitelné. Stejná služba vytvoří také relační klíč pro utajenou komunikaci mezi klientem a serverem.

Nakonec klient pošle serveru získaný lístek. Informace od klienta a relační klíč pro jejich vzájemnou komunikaci je zašifrován veřejným klíčem serveru.



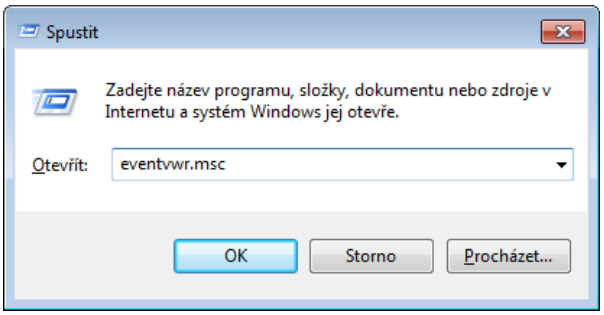
Tok požadavků a odpovědí při přihlášení do domény a při přístupu na server.

Kerberos je poměrně komplikovaný protokol, ale je velmi robustní a rozšiřitelný. Místo průchozí autentizace, kterou využívá protokol NTLM, je použit systém lístků, což autentizaci zrychluje. Kerberos umožňuje i tzv. tranzitivní důvěru v hierarchické struktuře domén.

VYBRANÉ POSTUPY KE ZKOUŠCE

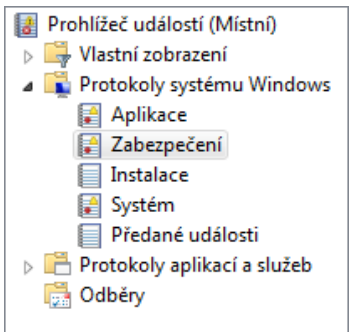
AUDIT OPERAČNÍHO SYSTÉMU

Nejjednodušší způsob jak vyvolat **Prohlížeč událostí**, pomocí kterého se audit provádí, je stisk kombinace kláves **Win + R,** zápis názvu nástroje **eventvwr.msc**, a stisk klávesy **Enter**.



Jinou možností pro vyvolání **Prohlížeče událostí** je kliknutí pravým tlačítkem myši na ikonu **Počítač** a výběr funkce **Spravovat**. V nástroji **Správa počítače**, který tak vyvoláme, je **Prohlížeč událostí** jedním ze zásuvných modulů.

Po spuštění **Prohlížeče událostí** klikneme vlevo na **Protokoly systému Windows**.

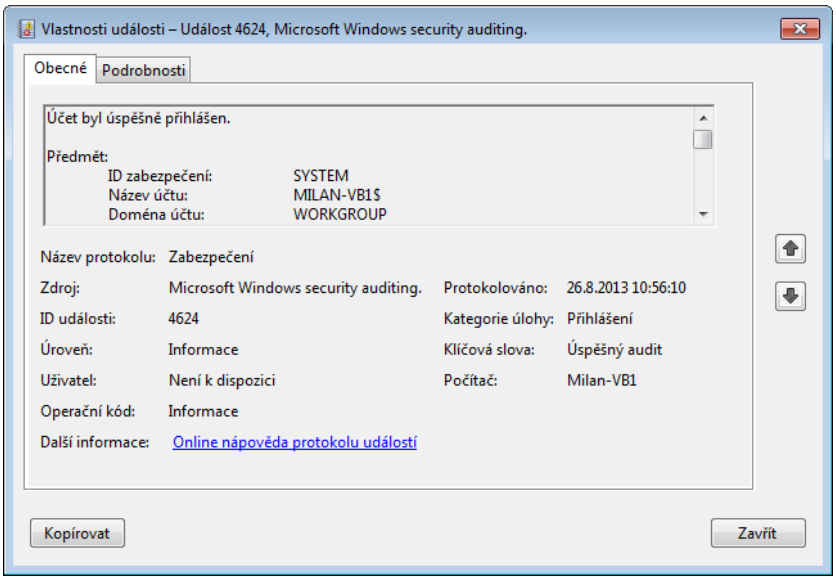


Události související s bezpečností operačního systému, které administrátora zajímají nejvíce, se zaznamenávají do protokolu **Zabezpečení**. Kromě něj existuje ještě protokol **Aplikace**, do kterého zaznamenávají události některé ze spuštěných aplikací, a protokol **Systém**, který využívá samotný operační systém - například k zápisu informací o průběhu svého spouštění, zavádění ovladačů a spouštění služeb. Další protokoly se vytvářejí v závislosti na roli, jakou počítač v síti plní.

Uprostřed okna **Prohlížeče událostí** se nachází seznam zaznamenaných událostí ve vybraném protokolu. U každé zaznamenané události slouží ikony vlevo k rychlé orientaci: žlutý klíč označuje úspěšnou akci, žlutý zámek neúspěšnou. Samostatné ikony má **Informace**, **Upozornění** a **Chyba**.

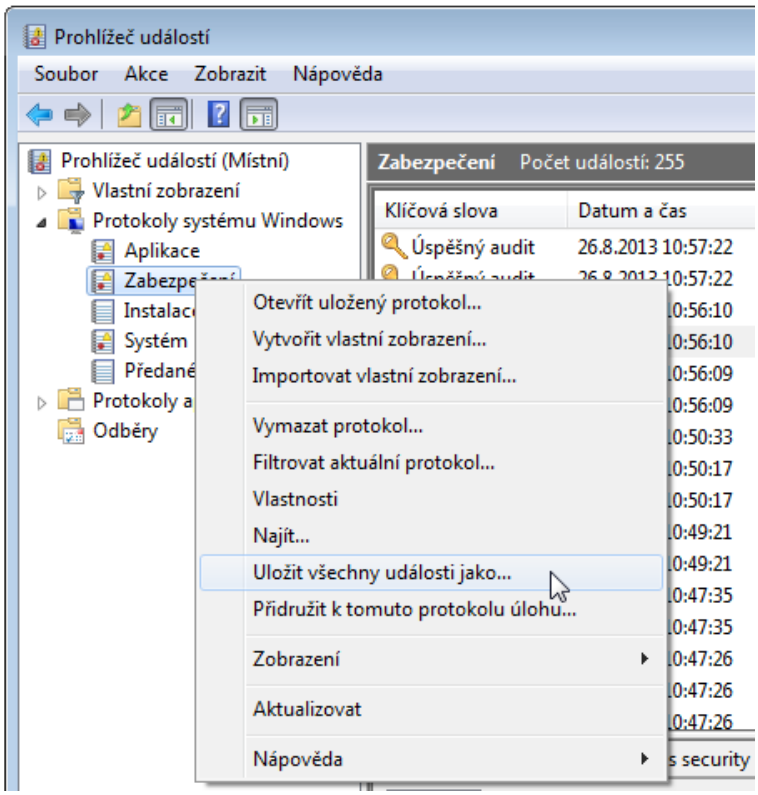
Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	26.8.2013 10:57:22	Microsoft Windows security auditing.	4905	Změna zásad auditu
Úspěšný audit	26.8.2013 10:57:22	Microsoft Windows security auditing.	4904	Změna zásad auditu
Úspěšný audit	26.8.2013 10:56:10	Microsoft Windows security auditing.	4672	Zvláštní přihlášení
Úspěšný audit	26.8.2013 10:56:10	Microsoft Windows security auditing.	4624	Přihlášení
Úspěšný audit	26.8.2013 10:56:09	Microsoft Windows security auditing.	4672	Zvláštní přihlášení
Úspěšný audit	26.8.2013 10:56:09	Microsoft Windows security auditing.	4624	Přihlášení
Úspěšný audit	26.8.2013 10:50:33	Microsoft Windows security auditing.	4616	Změna stavu zabezpeč...

U každé události se dále standardně zobrazuje datum a čas vzniku události, zdroj události, číselný identifikátor události a kategorie události. Zejména ID události se v praxi často používá; například k filtrování událostí. Dvojklikem na událost vyvoláme dialogové okno s podrobnou informací.



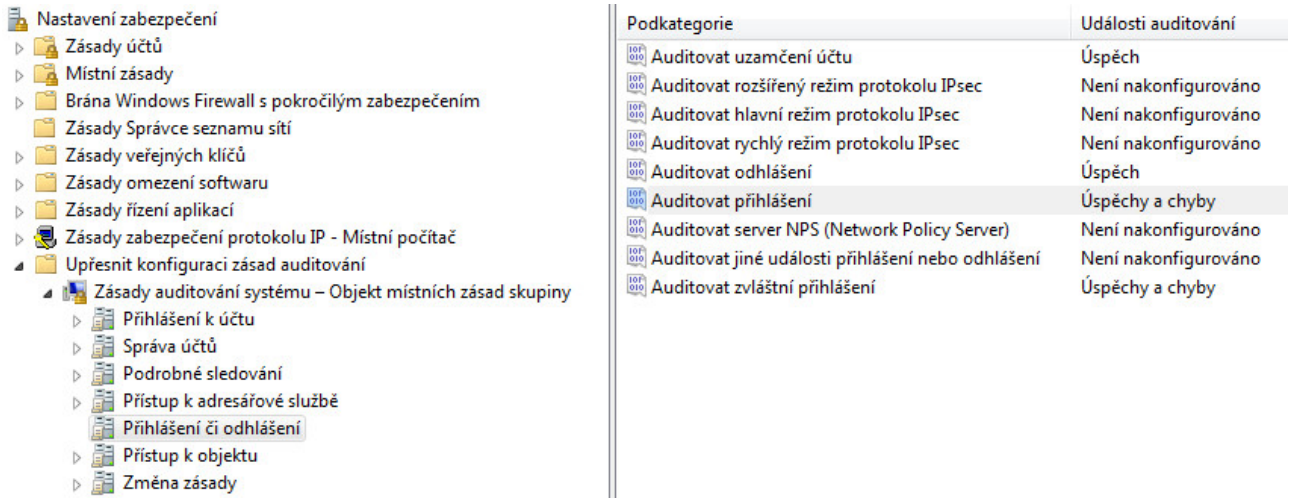
Bezpečnostní politika zpravidla definuje pro provádění auditu několik různých požadavků. Jednotlivé protokoly se například musí pravidelně analyzovat, zálohovat a uchovávat až několik let nazpátek. Kliknutím pravého tlačítka myši na jednotlivých protokolech vyvoláme kontextovou nabídku. Z kontextové nabídky se pak nejčastěji používá funkce pro uložení událostí do souboru na výměnném

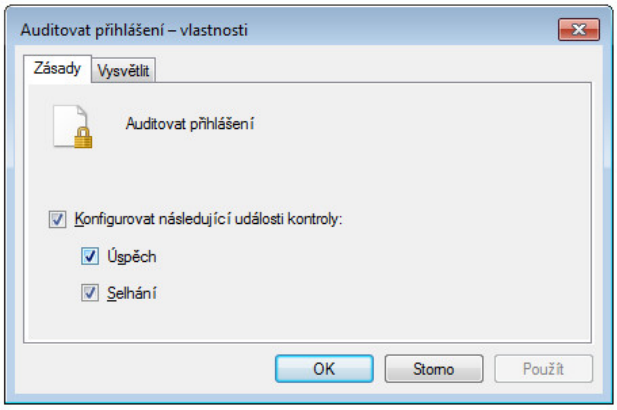
médiu, následně funkce pro vymazání protokolu, a otevření uloženého protokolu. Po vymazání protokolu **Zabezpečení** se do něj automaticky zaznamená událost 1102 – Vymazání prokolu, a to proto, aby ani administrátor po sobě nemohl smazat všechny stopy v systému.



Některé z událostí se začnou zanamenávat do příslušných protokolů hned po instalaci, ale o obsahu protokolu **Zabezpečení** rozhoduje především administrátor. Nejprve je třeba spustit potřebný nástroj. Stiskneme klávesy **Win + R,** zapíšeme název nástroje **secpol.msc**, a stiskneme klávesu **Enter**.
V nástroji **Místní zásady zabezpečení** vybereme vlevo uzel **Upřesnit konfiguraci zásad auditování → Zásady auditování systému**, a vpravo se zobrazí několik různých podkategorií událostí.

Sledování událostí spadajících do některé z podkategorií nastavíme dvojklikem na název podkategorie. V dialogovém okně pak zapneme sledování úspěšných nebo neúspěšných pokusů. Například můžeme zapnout položky **Přihlášení či odhlášení → Auditovat přihlášení**.

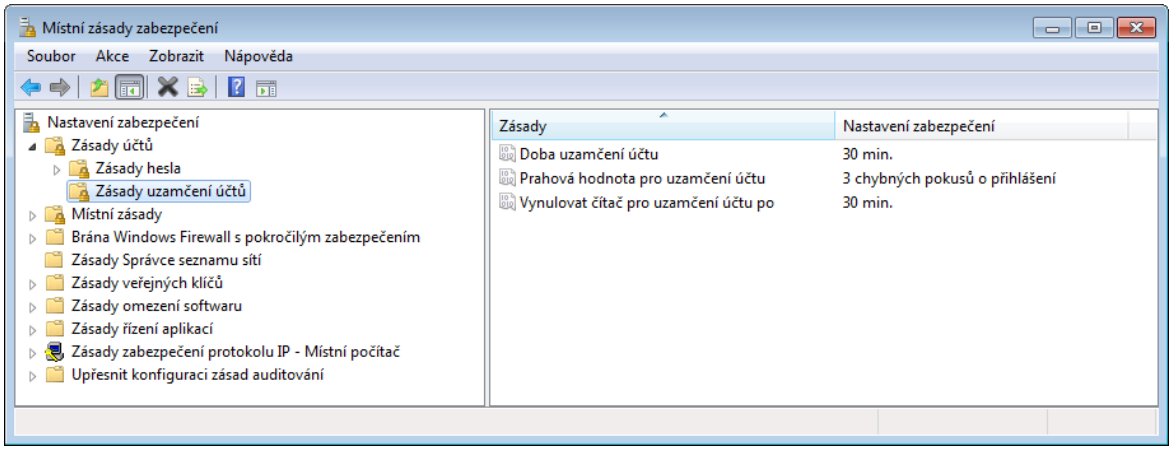




Pokud chceme sledovat přístup k objektům, jako jsou soubory, adresáře, tiskárny a klíče registru, musí být nejprve povolena kategorie událostí **Přístup k objektu**, a podkategorie např. **Auditovat systém souborů** (Úspěch a Selhání). To ale nestačí, ještě je třeba upravit u zvolených objektů jejich systémový ACL.

Pro ilustraci analýzy událostí si ukážeme typickou posloupnost zaznamenaných událostí odpovídající neúspěšnému přihlášení s následným uzamčením účtu, což odpovídá situaci, kdy si oprávněný uživatel nemůže vzpomenout na správné heslo.

Následující dialogové okno obsahuje parametry definující podmínky pro uzamčení uživatelských účtů. Doba uzamčení účtu je 30 minut, což znamená, že pokud už k uzamčení účtu dojde, po uplynutí 30 minut se tento účet sám odemkne. V praxi se ale za bezpečné nastavení považuje interval 0 minut, který ve skutečnosti znamená, že účet se neodemkne automaticky a sám, ale teprve po zásahu administrátora.

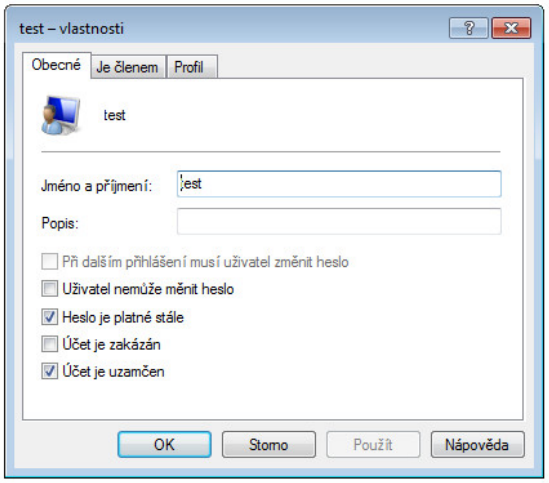


V protokolu zabezpečení tomu odpovídají události 4625, nejprve tři neúspěšná přihlášení a nakonec uzamčení účtu. Dále je v seznamu patrné i následné úspěšné přihlášení administrátora (ID 4624), který provádí analýzu auditu.

Zabezpečení Počet událostí: 18

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	9.1.2018 14:36:26	Eventlog	1102	Vymazání protokolu
Úspěšný audit	9.1.2018 14:36:37	Microsoft Windows security auditing.	4647	Odhlášení
Neúspěšný audit	9.1.2018 14:36:42	Microsoft Windows security auditing.	4625	Přihlášení
Neúspěšný audit	9.1.2018 14:36:45	Microsoft Windows security auditing.	4625	Přihlášení
Neúspěšný audit	9.1.2018 14:36:47	Microsoft Windows security auditing.	4625	Přihlášení
Úspěšný audit	9.1.2018 14:36:47	Microsoft Windows security auditing.	4740	Správa uživatelských účtů
Neúspěšný audit	9.1.2018 14:36:49	Microsoft Windows security auditing.	4625	Uzamčení účtu
Neúspěšný audit	9.1.2018 14:36:55	Microsoft Windows security auditing.	4625	Uzamčení účtu
Úspěšný audit	9.1.2018 14:37:04	Microsoft Windows security auditing.	4648	Přihlášení
Úspěšný audit	9.1.2018 14:37:04	Microsoft Windows security auditing.	4672	Zvláštní přihlášení
Úspěšný audit	9.1.2018 14:37:04	Microsoft Windows security auditing.	4624	Přihlášení
Úspěšný audit	9.1.2018 14:37:04	Microsoft Windows security auditing.	4624	Přihlášení

Odemčení účtu se provede pomocí nástroje **Místní uživatelé a skupiny** (lusrmgr.msc). Stačí vypnout zaškrtávací pole **Účet je uzamčen**.



LUŠTĚNÍ HESEL UŽIVATELSKÝCH ÚČTŮ WINDOWS

V SAM databázi se standardně ukládá už jen NTLM hash hesla, takže pokud chceme útočit i na slabší LM hash, povolíme ukládat LM hash dle postupu z kapitoly Autentizační protokoly Windows. Pokud máme přístup k administrátorskému účtu, tak je pro přečtení hash hodnot hesel nejjednodušší použít nástroje jako fgdump, pwdump6 (http://foofus.net/goons/fizzgig/) nebo pwdump7 (http://www.tarasco.org/security/tools.html).

Například pwdump6 spuštěný s parametry **pwdump -x localhost** vrátí mimo jiné následující seznam účtů: (-x je určené pro 64 bitové Windows , localhost identifikuje jako cíl místní počítač)

```
Administrator:500:NO PASSWORD**********************:NO PASSWORD**********************:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
test1:1005:5E4EB528699CD4B01F3F516BF8D0BF04:B3D60CDDE5942F8A4E781C3FD04535D7:::
test2:1006:3D1CF71B7EBADB986C49BF00DCE36B32:8FC3AE035101A0B1061B8774F6D7D5EA:::
test3:1007:C782FC1FFB111AA7C9402FF13538DA54:77070D86D48DAC14E745240D9278863E:::
```

Formát seznamu je docela jednoduchý. Za jménem účtu je relativní identifikátor, LM hash a NTLM hash, dvojtečky slouží jako oddělovač. Zaměříme se na účty test1 až test3 a k útoku na LM hash použijem např. hashcat (https://hashcat.net/hashcat/).

```
hashcat64 -m 3000 -a 3 5E4EB528699CD4B01F3F516BF8D0BF04
```

(Parametr -m 3000 určuje útok na LM hash, -a 3 znamená útok hrubou silou, tj. budou se zkoušet všchny možné kombinace)

Vyluštěná hesla se automaticky zapisují do souboru hashcat.potfile, kde najdeme

```
1f3f516bf8d0bf04:ADNE
```

```
5e4eb528699cd4b0:HESL8SN
```

Tzv. LM heslo je tedy řetězec `HESL8SNADNE`, skutečné heslo obsahuje 11 znaků a bude se lišit jen tím, že některé znaky budou malé.

```
hashcat64 -m 1000 -a 3 B3D60CDDE5942F8A4E781C3FD04535D7 -1 HhEeSsLl8NnAaDd ?1?1?1?1?1?1?1?1?1?1?1
```

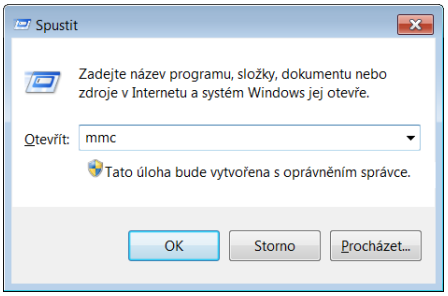
(Parametr -m 1000 určuje útok na NTLM hash, -a 3 znamená útok hrubou silou,-1 definuje vlastní znakovou sadu, kterou vytvoříme z již známého LM hesla. Na konci je uvedena maska, dle které hashcat bude generovat jedenáctiznakové kombinace z námi definované znakové sady.)

Asi po třiceti minutách se objeví vyluštěné heslo `b3d60cdde5942f8a4e781c3fd04535d7:Hesl8Snadne`.

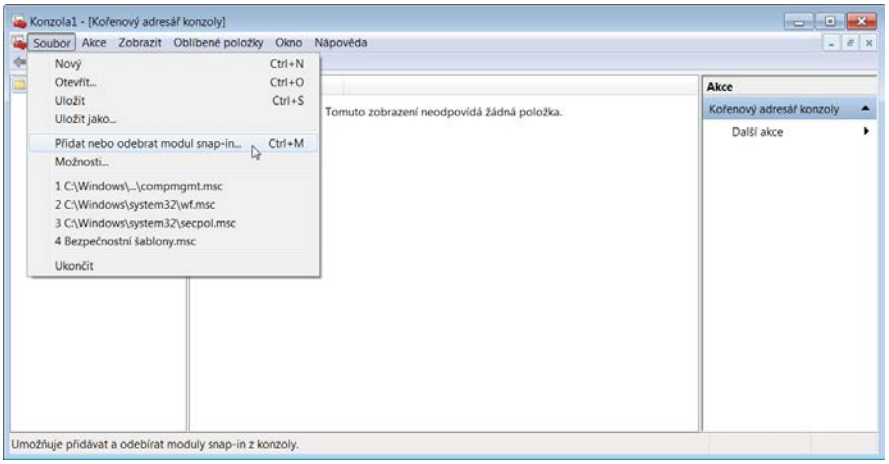
KONFIGURACE WINDOWS POMOCÍ BEZPEČNOSTNÍ ŠABLONY

Správná konfigurace Windows znamená pro administrátora provést až stovky drobných zásahů, což lze s vhodným nástrojem automatizovat. Na rozdíl od administrátorských nástrojů, které jsou k dispozici hned po instalaci, je ovšem nutné zmíněný nástroj nejprve vytvořit. Provede se to tak, že do prázdné MMC konzoly přidáme dva vybrané zásuvné moduly.

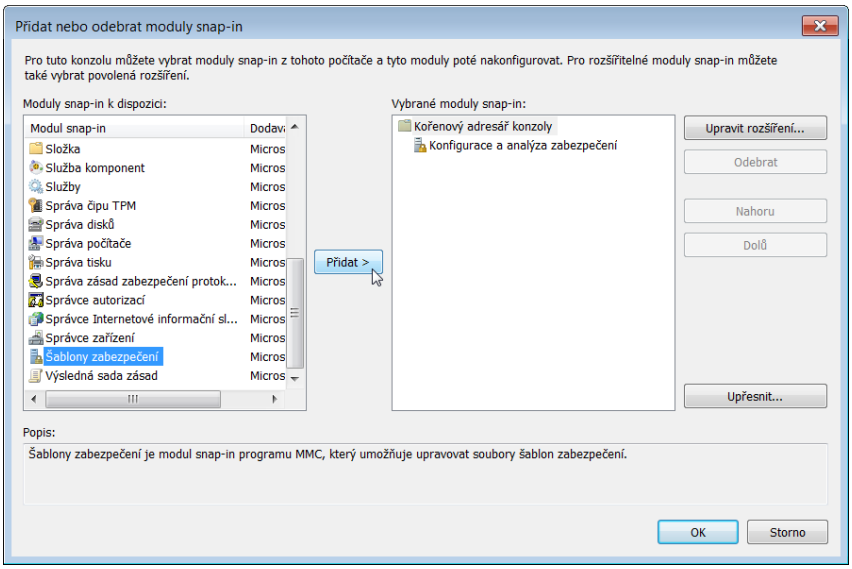
Nejjednodušší způsob jak vyvolat **MMC konzolu** je stisk kombinace kláves **Win + R,** zápis názvu nástroje **mmc**, a stisk klávesy **Enter**.



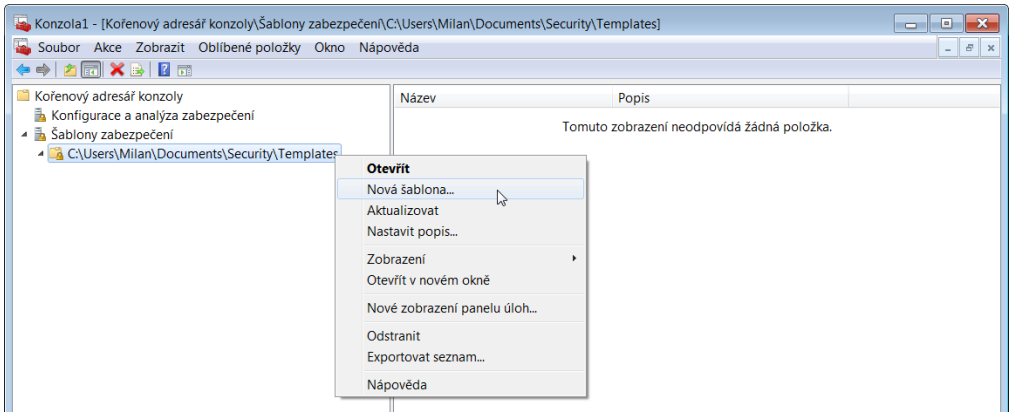
V menu Soubor vybereme příkaz **Přidat nebo odebrat modul snap-in**.



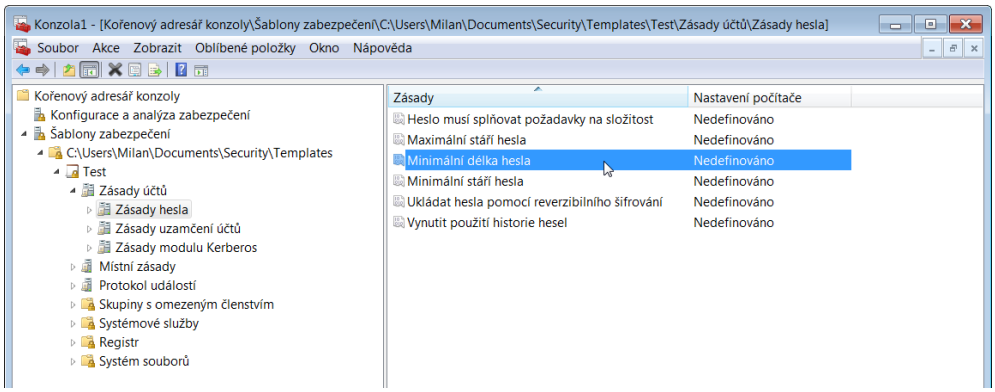
A přidáme postupně dva zásuvné moduly: **Šablony zabezpečení** a **Konfigurace a analýza zabezpečení**. Po přidání obou modulů stiskneme tlačítko **OK**.



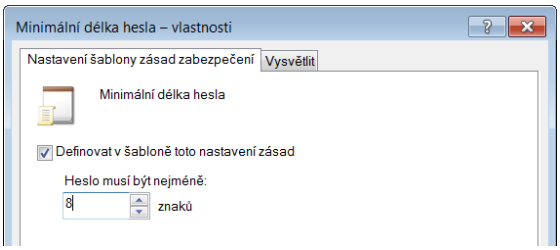
Klikneme na uzel **Šablony zabezpečení** a vytvoříme v implicitním adresáři pro ukládání šablon novou šablonu, kterou pojmenujeme například test.



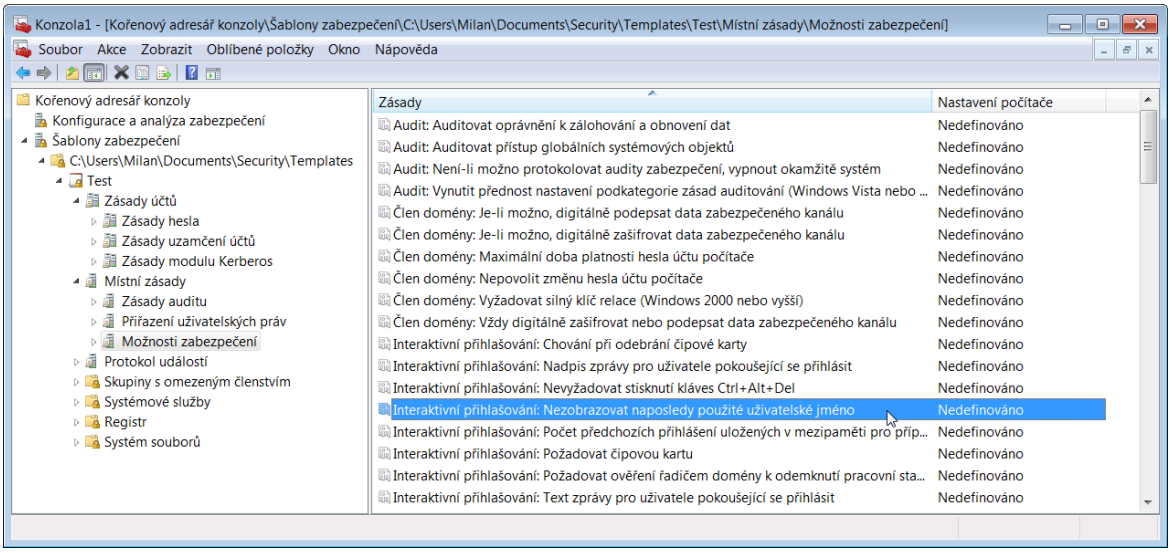
Takto vytvořená šablona obsahuje stovky různých parametrů, které jsou ale v počátečním stavu nedefinovány. Chceme-li například změnit minimální délku hesla, vybereme nejprve ten správný parametr dle následujícího obrázku.



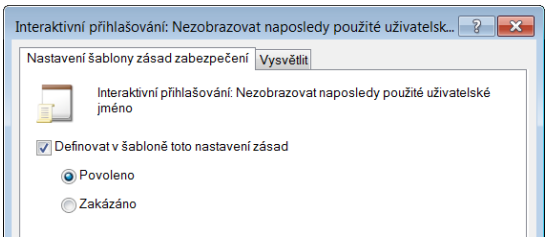
Dvojklikem na parametr nejprve zaškrtneme položku **Definovat v šabloně toto nastavení zásad** a poté nastavíme minimální délku hesla například na 8 znaků.



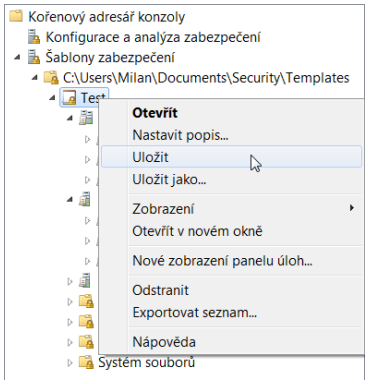
Pokud by chtěl administrátor zakázat zobrazování posledního přihlášeného uživatele, opět si nejprve vybere ten správný parametr.



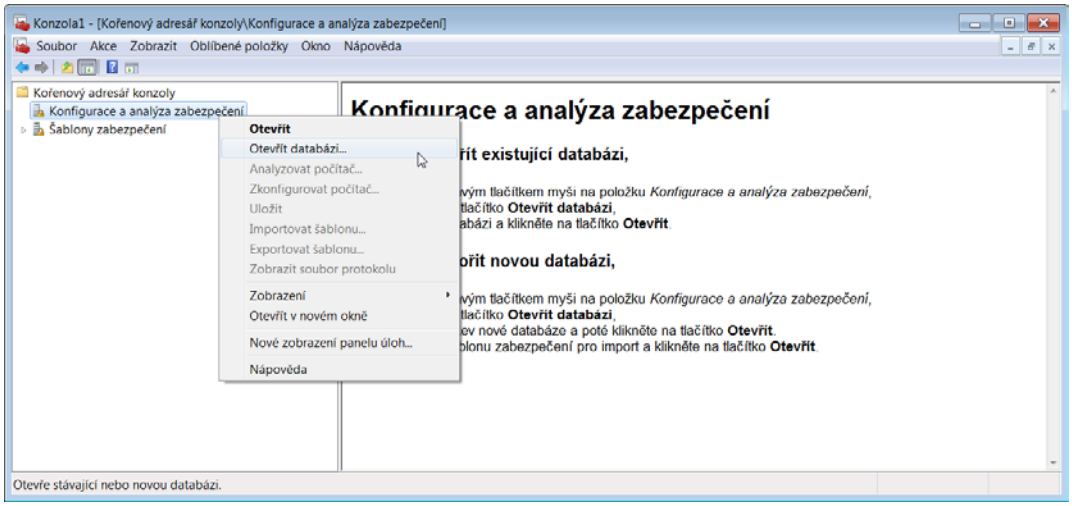
A dvojklikem nastaví požadovaný stav parametru. V tomto případě stav **Povoleno** znamená, že se poslední přihlášený uživatel nebude zobrazovat.



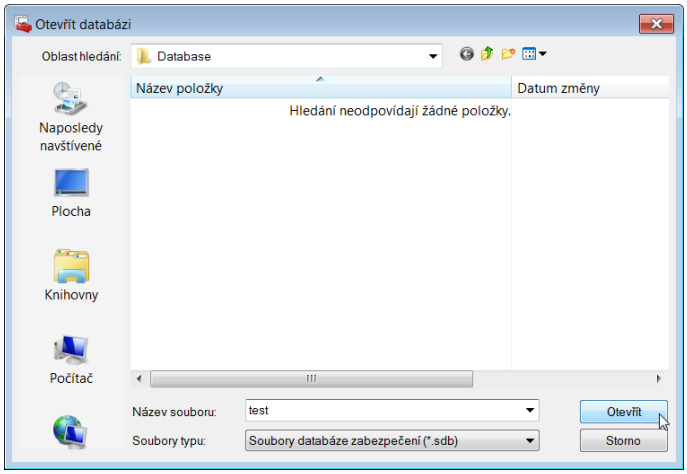
Po úpravě všech potřebných parametrů je potřeba provedené změny uložit tak, že klikneme pravým tlačítkem myši na název šablony a vybereme příkaz **Uložit**.



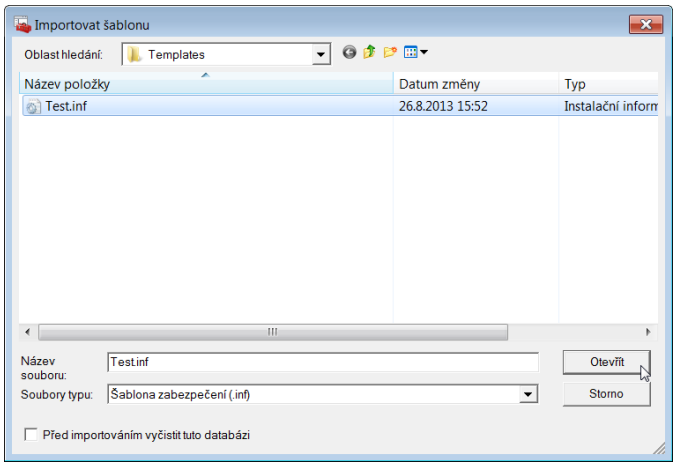
Parametry uložené v šabloně nyní načteme do databáze, kterou si za tímto účelem vytvoříme. Nejprve klikneme na uzel **Konfigurace a analýza zabezpečení**, kde vybereme příkaz **Otevřít databázi**.



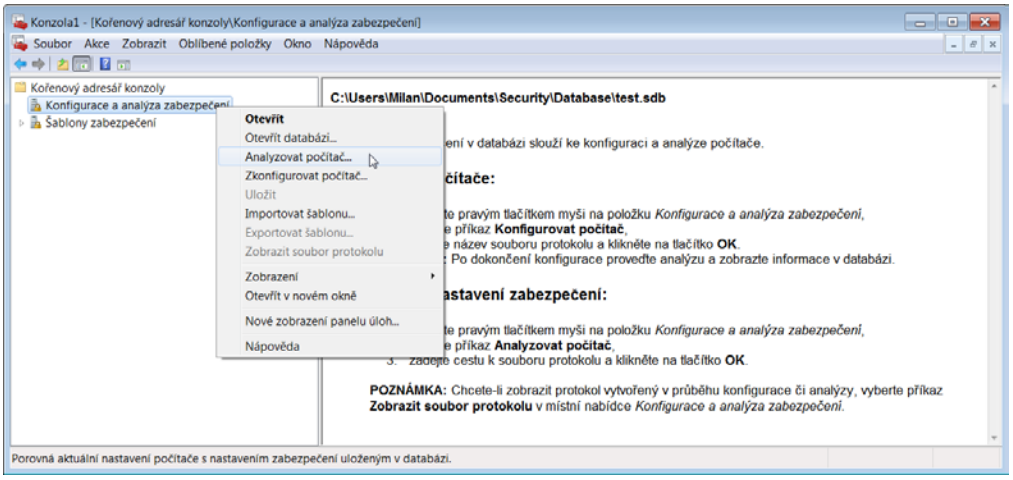
V dialogovém okně do pole **Název souboru** zapíšeme jméno vytvářené databáze, například test.



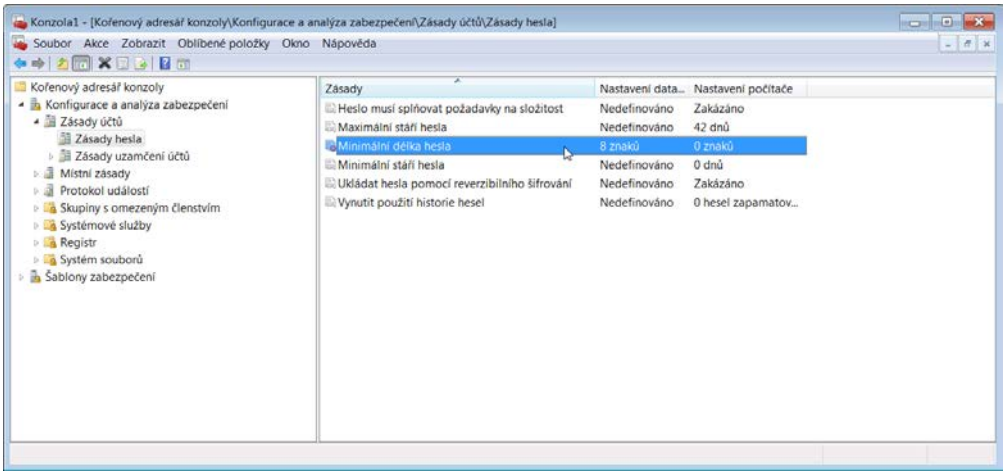
A do databáze naimportujeme parametry z naší bezpečnostní šablony.



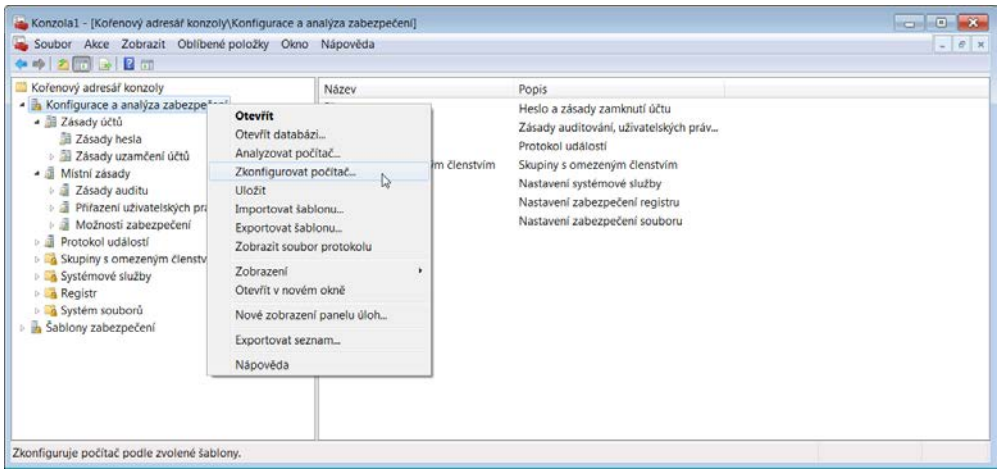
Pomocí databáze test můžeme nyní provést porovnání stávající konfigurace počítače s konfigurací, kterou jsme si připravili v bezpečnostní šabloně. Klikneme pravým tlačítkem myši na uzel **Konfigurace a analýza zabepečení** a vybereme příkaz **Analyzovat počítač**. Průběh analýzy se zaznamená do souboru test.log, který můžeme později použít k odladění šablony.



Výsledek analýzy se zobrazí ve stejné hierarchické podobě, jakou měly parametry v bezpečnostní šabloně. Rozklikneme uzel **Konfigurace a analýza zabepečení** a podíváme se na dva parametry, které jsme v bezpečnostní šabloně změnili. Pomocí ikon jsme schopni jednoduše a rychle odlišit odchylky v obou konfiguracích.



Pokud jsme spokojeni s výsledkem analýzy, můžeme nyní vynutit změny, které jsme si při analýze vyzkoušeli nanečisto. Klikneme pravým tlačítkem myši na uzel **Konfigurace a analýza zabepečení** a vybereme příkaz **Zkonfigurovat počítač**.



Bezpečnostní šablonu (test.inf) můžeme snadno přenést na jiný počítač, takže můžeme dosáhnout toho, že všechny vybrané počítače budou shodně konfigurovány.