KAPITOLA 4

Bezpečnostní nástroje

V této kapitole:
- AccessChk, AccessEnum
- Autologon, Autoruns
- Msconfig, LogonSessions
- PsExec, PsLoggedOn
- PsLogList, RootkitRevealer
- SDelete, ShareEnum
- ShellRunas, Runas
- SigCheck, SigVerif
- Verifier

V této kapitole budou blíže představeny utility Sysinternals z kategorie Security Tools. Jedná se o nástroje zaměřené na testování a diagnostiku, správu a konfiguraci zabezpečení systému Windows. Některé z popisovaných nástrojů najdou uplatnění při bezpečnostních testech softwaru a nastavení operačního systému Windows.

Kapitola o bezpečnostních utilitách přináší například informace o kontrole přístupových práv, typech rootkitů, možnostech zrychlování spouštěcího procesu operačního systému Windows nebo způsobech bezpečného odstraňování souborů z pevného disku.

Následující text blíže představuje tyto nástroje:

SYSINTERNALS:

- AccessChk
- AccessEnum
- Autologon
- Autoruns
- LogonSessions
- PsExec
- SigCheck
- PsLogList
- PsLoggedOn
- RootkitRevealer
- SDelete
- ShareEnum
- ShellRunas

OSTATNÍ:

- Msconifg
- Runas
- SigVerif

AccessChk

Název:	AccessChk	
Velikost:	110 kB	
Kategorie:	Security tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb664922*	

Popis

Nástroj AccessChk umožňuje síťovým administrátorům získávat informace o přístupových právech. Mezi informace, které lze na výstupu aplikace získat, je typ přístupových práv pro konkrétní uživatele nebo uživatelské skupiny k souborům, adresářům, službám systému Windows, registrovým klíčům nebo globálním objektům.

Použití

```
accesschk [-s][-e][-u][-r][-w][-n][-v][[-a]|[-k]|[-p [-f] [-t]]
          [-o [-t <object type>]][-c]|[-d]] [[-l [-i]]|[username]]
          <file, directory, registry key, process, service, object>
```

Seznam podporovaných parametrů

`-a`	Jméno přístupového práva Windows. Použitím zástupného znaku hvězdičky „`*`“ se zobrazí všechny účty přiřazené k právu. Při specifikování konkrétního přístupového práva se ve výpisu zobrazí jen uživatelský účet nebo skupina, která je přiřazena k danému právu.
`-c`	Jméno služby Windows, například jako SNMPTRAP. Pokud se místo jména zadá zástupný znak hvězdičky „`*`“, zobrazí se seznam přístupových práv pro všechny služby.
`-d`	Zpracování adresářů nebo nejvyšší úrovně klíčů.
`-e`	Zobrazení jen explicitně uvedených úrovní integrity (podporované jen na Windows Vista a vyšších).
`-f`	Zobrazení všech informací včetně skupin a práv.
`-k`	Jméno registrového klíče, například `hklm\software`.
`-i`	Ignorování zděděných položek řízení přístupu (Access Control Entries, ACE). Tento parametr lze používat při výpisu plných přístupových seznamů.
`-l`	Zobrazení plného přístupového seznamu. Použitím parametru `-i` se ignorují zděděné položky řízení přístupu.
`-n`	Zobrazení jen objektů, které nemají přístupová práva.
`-o`	Jméno objektu v Object Manager namespace (předvolené je `root`). K prohlížení obsahu adresářů je potřeba specifikovat jméno se zpětným lomítkem na konci, nebo přidat parametr `-s`. Přidáním parametru `-t` a definováním typu objektu (například `Section`) se zobrazí jen objekty specifikovaného typu.

`-p`	Jméno nebo PID procesu, například cmd.exe (použitím zástupného znaku hvězdičky „*" namísto jména se zobrazí všechny procesy). Tento parametr lze používat spolu s parametrem `-f`, který umožní zobrazení plných informací o skupinách a právech. Dalším parametrem, který je možné přidat, je `-t`. Tento parametr zobrazí vlákna.
`-q`	Vynechání banneru ve výpisu výstupu.
`-r`	Zobrazení jen objektů, které mají přístup pro čtení.
`-s`	Rekurze.
`-t`	Filtrování objektů (například `Section`).
`-u`	Potlačení chyb.
`-v`	Rozšíření výstupních informací (včetně Windows Vista Integrity Level – viz Poznámku).
`-w`	Zobrazení jen objektů, které mají přístup pro zápis.

Poznámka: Windows Vista Integrity Level je komponenta bezpečnostní architektury systému Windows, která umožňuje omezovat přístupová práva aplikací, které běží pod stejným uživatelským účtem, ale mají přiřazenou nižší důvěryhodnost. Například neznámý, potenciálně nebezpečný kód stažený z Internetu má zabráněno měnit systémová nastavení, uživatelská data nebo manipulovat jinými aplikacemi. Podrobnější informace o této komponentě najdete na stránkách projektu MSDN (*http://msdn.microsoft.com/en-us/library/bb625957.aspx*).

Příklady použití

Nástroj v základním použití vypisuje přístupová práva pro objekty, které mají nastavené právo čtení a zápisu. V případě, že testovaný objekt nemá specifikovaná žádná z těchto práv, bude výpis prázdný.

1. Testování přístupových práv čtení a zápisu pro konkrétního uživatele (*NovakM*) k souborům a adresářům v systémovém adresáři:

```
accesschk NovakM c:\windows

RW c:\windows\addins
RW c:\windows\AppCompat
RW c:\windows\AppPatch
RW c:\windows\ARJ.PIF
RW c:\windows\assembly
RW c:\windows\atiogl.xml
RW c:\windows\ativpsrm.bin
R  c:\windows\bfsvc.exe
RW c:\windows\camcodec100.ini
RW c:\windows\cs
RW c:\windows\CSUP.txt
RW c:\windows\Cursors
```

2. Otestování, kdo v systému má právo změnit nastavení času:

```
accesschk -a SeInteractiveLogonRight

  S-1-5-32-551
```

```
BUILTIN\Users
BUILTIN\Administrators
VIAGROS-HP\Guest
VIAGROS-HP\__vmware__
```

3. Zobrazení přístupových práv ke službě SkypeUpdate:

```
accesschk -c SkypeUpdate -q

SkypeUpdate
RW NT AUTHORITY\SYSTEM
RW BUILTIN\Administrators
R  NT AUTHORITY\INTERACTIVE
R  NT AUTHORITY\SERVICE
```

Využití

Nástroj je určen pro systémové administrátory, kteří potřebují mít přehled o přístupových právech uživatelů síťové infrastruktury. Nástroj mohou používat například i analytici při bezpečnostním auditu firemní sítě.

AccessEnum

Název:	AccessEnum	
Velikost:	51 kB	
Kategorie:	Security tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb897332*	

Popis

Utilita AccessEnum umožňuje kontrolovat a vypisovat přístupová práva k souborům, adresářům a registrovým klíčům. Specifickou vlastností této utility je, že ve výpisu testovaných objektů uvádí jen rozdílná přístupová práva ve srovnání s nadřazeným (rodičovským) objektem. Pro názornost je níže popsán postup práce s utilitou a ukázka výpisu. AccessEnum testuje 3 druhy přístupových práv – čtení, zápis, zablokovaný přístup.

Jednou z výhod aplikace je i možnost exportu výsledků testu, který lze případně použít k dalšímu zpracování, nebo jen pro archívní účely.

Příklady použití

Je potřeba otestovat přístupová práva v adresářové struktuře:

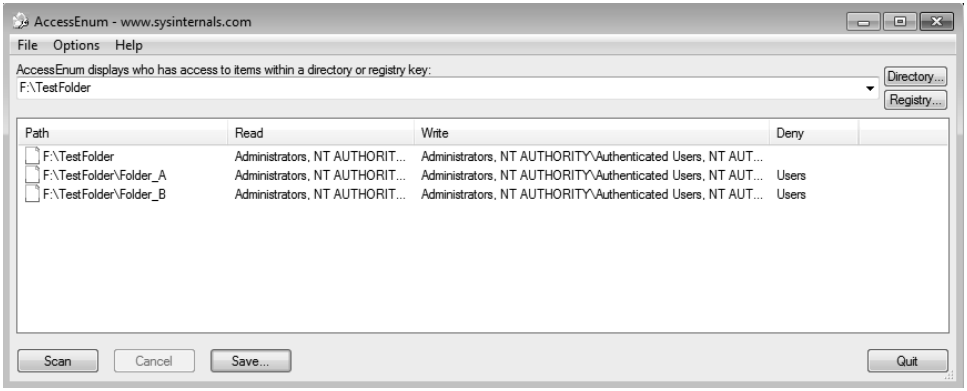
- *TestFolder*

- *Folder_A*
- *Folder_B*
- *Folder_C*

Otestování nastavených přístupových práv k adresáři zahrnuje:

1. Spuštění utility AccessEnum.
2. Vložení cesty k testovanému adresáři *TestFolder* do adresního řádku.
3. Klepnutí na tlačítko **Scan**.

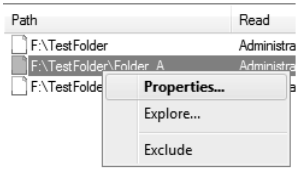
Následně dojde k otestování přístupových práv. Výsledek se zobrazí formou výpisu, jaký je vyobrazen na obrázku 4.1. Výpis informuje o právech rodičovského adresáře *TestFolder* (první řádek výpisu), adresáře *Folder_A* a *Folder_B* (druhý a třetí řádek výpisu) jsou vypsány, protože obsahují odlišné nastavení přístupových práv než rodičovský adresář (Deny přístup pro účet User). Poslední adresář *Folder_C* se ve výpisu nezobrazí, protože má stejné nastavení přístupových práv jako rodičovský adresář *Folder*.



Obrázek 4.1 AccessEnum

Klepnutím pravým tlačítkem myši na řádek výpisu se zobrazí místní nabídka se třemi volbami (viz obrázek 4.2). Tyto volby umožňují:

- zobrazení vlastností testovaného adresáře (volba **Properties**);
- procházení adresáře (volba **Explore**);
- odstranění řádku z výsledku, ignorování výsledků (volba **Exclude**).



Obrázek 4.2 AccessEnum – místní nabídka

Utilita AccessEnum umožňuje testovat také registrové klíče. Prostřednictvím tlačítka **Registry** je možné vyvolat dialog, který zobrazí okno pro procházení struktury systémových registrů.

Získané výsledky testování je možné uložit v textovém formátu. Export výsledků testu je vhodné použít například v situacích, kdy je zapotřebí získat přístupová práva jednotlivých souborů umístěných v testovaných adresářích.

Výsledný soubor obsahuje řadu informací, které se mohou zdát na první pohled nepřehledné. V hlavičce souboru je možné vidět legendu, která vysvětluje, co znamenají jednotlivé záznamy mezi uvozovkami (`Path` – cesta, `Read` – právo čtení, `Write` – právo zápisu, `Deny` – zamítnutý přístup). Následně je na každém řádku zapsán výsledek testu jednoho souboru, případně adresáře:

```
"Path"  "Read"  "Write"  "Deny"
"C:\Windows"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller, Users"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller"
  ""
"C:\Windows\addins\FXSEXT.ecf"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller, Users"
  "NT SERVICE\TrustedInstaller"
  ""
"C:\Windows\AppCompat\Programs\RecentFileCache.bcf"
  "Administrators, NT AUTHORITY\SYSTEM"
  "Administrators, NT AUTHORITY\SYSTEM"
  ""
"C:\Windows\AppPatch\AcGenral.dll"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller, Users"
  "NT SERVICE\TrustedInstaller"
  ""
"C:\Windows\AppPatch\AcLayers.dll"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller, Users"
  "NT SERVICE\TrustedInstaller"
  ""
"C:\Windows\AppPatch\AcRes.dll"
  "Administrators, NT AUTHORITY\SYSTEM, NT SERVICE\TrustedInstaller, Users"
  "NT SERVICE\TrustedInstaller"
  ""
```

Následující upravený výpis demonstruje, jak je potřeba číst soubor obsahující export výsledků:

```
"Path" – "C:\Windows"
"Read" – "Administrators, NT AUTHORITY\SYSTEM,
  NT SERVICE\TrustedInstaller, Users"
"Write" – "Administrators, NT AUTHORITY\SYSTEM,
  NT SERVICE\TrustedInstaller"
"Deny" – ""
```

Využití

Tato utilita najde uplatnění například při vývoji a testování softwarových aplikací. Tyto aplikace musejí mít po instalaci do systému nastavená přístupová práva k jednotlivým adresářům. V případě jejich nesprávného nastavení by například uživatelé nemohli zapisovat do protokolů, měnit konfiguraci aplikace atd. Prostřednictvím AccessEnum je možné relativně rychle najít nesprávně nastavená přístupová práva. Manuální kontrola přístupových práv každého sou-

boru a adresáře jednotlivě by byla časově náročná a existuje tu poměrně velké riziko selhání lidského faktoru, který by mohl některá chybná nastavení přehlédnout.

Autologon

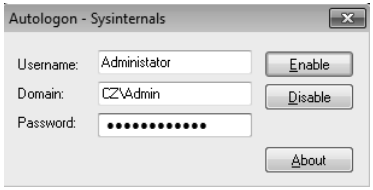
Název:	Autologon	
Velikost:	76,9 kB	
Kategorie:	Security tools	
Typ utility:	GUI	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb963905*	

Popis

Pomocí tohoto nástroje je možné konfigurovat funkci Autologon, která je běžnou součástí operačního systému Windows. Funkce Autologon umožňuje, aby uživatel nemusel při každém spuštění počítače zadávat přihlašovací jméno a heslo. Tato utilita je vhodná zejména tam, kde stanici používá jeden uživatel, a neexistují rizika odcizení citlivých údajů. Vhodné je to například pro domácí uživatele.

Upozornění: Ve firemním prostředí, kde jsou na stanicích a síťových úložištích uloženy citlivé údaje, ať už o zákaznících nebo projektech, není vhodné tuto funkci používat. Firma se totiž tímto vystavuje riziku ztráty, respektive neoprávněného získání dat třetí osobou.

Utilita obsahuje jednoduché grafické rozhraní (obrázek 4.3), prostřednictvím něhož lze specifikovat konkrétního uživatele, doménu a heslo, které se má použít při automatickém přihlášení.



Obrázek 4.3 Autologon

Konfigurace automatického přihlášení vyžaduje definování uživatelského jména, hesla, případně domény, pokud se jedná o doménový účet. Po zadání požadovaných přihlašovacích údajů je potřeba pomocí tlačítka **Enable** toto nastavení uložit.

Pokud je potřeba do systému přihlásit jiného uživatele, během bootování systému Windows je nutné držet stisknutou klávesu Shift, která zobrazí klasický přihlašovací dialog, kde lze opět zadat libovolné přihlašovací jméno, heslo, případně doménu.

Využití

Jak už bylo uvedeno výše, tato aplikace najde uplatnění hlavně u domácích uživatelů. Ve firemním prostředí není její použití (povolení automatického přihlašování do systému) příliš

vhodné. Představuje to přemostění bezpečnostního opatření – přihlašovacího mechanismu. V případě krádeže zařízení (například notebooku) má útočník otevřenou cestu do systému.

Autoruns

Název:	Autoruns	
Velikost:	536 kB	
Kategorie:	Security tools	
Typ utility:	CMD, GUI	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb963902*	

Popis

Utilita Autoruns je velmi komplexním nástrojem, který poskytuje informace a umožňuje správu služeb, aplikací, knihoven, ovladačů a dalších doplňků, které se spouštějí při bootování operačního systému nebo při přihlašování uživatele.

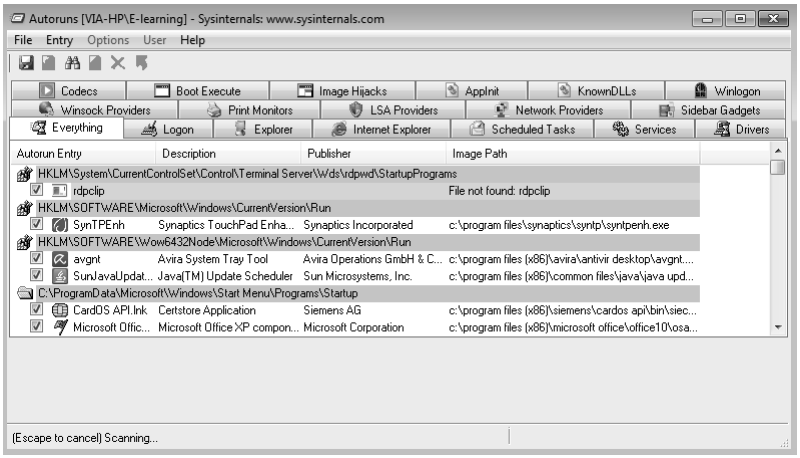
Nástroj umožňuje diagnostikovat problémy:

- Při spouštění systému – ovladače bránící, respektive znemožňující správné spuštění operačního systému.
- S rychlostí spouštění systému – při startu operačního systému, pokud se spouští příliš mnoho procesů, které se navíc snaží o kontrolu aktualizací po síti, může být samotný proces startu operačního systému zdlouhavý.
- Podezření na přítomnost škodlivého softwaru – škodlivý software se může automaticky přidat do seznamu aplikací, které se mají spouštět po startu. Tím může například získat kontrolu nad stanicí hned od začátku.

Tato utilita je dostupná ve dvou variantách. S grafickým rozhraním a ve formátu pro příkazový řádek. Po rozbalení archívu je možné najít dva soubory. *Autoruns.exe* je utilita s grafickým rozhraním, *Autorunsc.exe* je varianta utility pro příkazový řádek.

Autoruns.exe

Utilita ve variantě s grafickým rozhraním (*autoruns.exe*) po spuštění rozdělí všechny zjištěné informace o spouštěných knihovnách, aplikacích a modulech do osmnácti kategorií (viz obrázek 4.4). U jednotlivých položek je uveden název a cesta k souborům (knihovny, spustitelné soubory atd.), datum vytvoření souboru, v případě dostupnosti i krátký popis a jméno vydavatele, případně vlastníka souboru.



Obrázek 4.4 Autoruns

Tip: V předvoleném nastavení jsou systémové položky skryty. Zobrazíte je vypnutím volby skrývání systémových položek. Uvedené nastavení je možné vypnout v nabídce:

Options → Filter Options → Hide Windows entries

U jednotlivých položek v seznamech je možné klepnutím pravým tlačítkem myši vyvolat místní nabídku, která obsahuje rozšiřující volby. Místní nabídka obsahuje několik položek:

- **Delete** – vybraný záznam bude odstraněn (soubor nebude odstraněn, smaže se jen z vybraného seznamu).
- **Copy** – kopírování vybrané položky.
- **Jump to Entry** – přechod k dané položce v registrových záznamech (otevře se nové okno aplikace Regedit).
- **Jump to Image** – přechod k souboru zvolené položky (otevře se nové okno Průzkumníka s adresou aktuálního umístění zvolené položky).
- **Search Online** – vyhledávání informací na Internetu (ve verzi 11.34 tato funkce nefungovala správně).
- **Process Explorer** – propojení s utilitou Process Explorer.
- **Properties** – zobrazení vlastností zvolené položky.

Aplikace Autoruns umožňuje upravovat tato nastavení pro všechny uživatelské účty, které jsou na dané stanici vytvořeny. Změny nastavení pro jiný uživatelský účet je možné docílit přepnutím uživatele v aplikaci Autoruns. Samotné přepnutí realizujete volbou **User → Volba nového uživatele**.

Aplikace umožňuje export získaných informací ve formátu ARN (proprietární formát) a TXT.

Autorunsc.exe

Varianta aplikace Autorun pro příkazový řádek nabízí obdobné možnosti jako grafická verze s tím rozdílem, že navíc umožňuje export do formátů CSV a XML.

Použití Autorunsc.exe

```
autorunsc [-x] [[-a] | [-b] [-c] [-d] [-e] [-g] [-h] [-i] [-k] [-l]
          [-m] [-o] [-p] [-r] [-s] [-v] [-w]
          [[-z <systemroot> <userprofile>] | [user]]]
```

Seznam podporovaných parametrů

`-a`	Výpis všech záznamů (použití tohoto parametru vypíše několik desítek obrazovek záznamů).
`-b`	Výpis záznamů spouštěných při bootování systému.
`-c`	Tisk výstupu do formátu CSV.
`-d`	Výpis záznamů z kategorie Appinit DLL.
`-e`	Moduly k Exploreru (pozor, nikoliv Internet Exploreru).
`-g`	Informace o miniaplikacích (Vista a vyšší).
`-h`	Informace o Image Hijacks.
`-i`	Moduly a doplňky Internet Exploreru.
`-l`	Výpis záznamů spouštěných při přihlášení uživatele.
`-m`	Skrývání záznamů podepsaných Microsoftem.
`-n`	Informace o kategoriích Winsock Protocol a Network Providers.
`-p`	Výpis ovladačů tiskáren.
`-r`	Informace o kategorii LSA Providers.
`-s`	Seznam služeb spouštěných automaticky a nezablokovaných ovladačích.
`-r`	Naplánované úlohy.
`-v`	Ověření digitálních podpisů.
`-w`	Záznamy Winlogon.
`-x`	Tisk do formátu XML.
`-z`	Specifikování offline Windows systému, který má být skenován.
`user`	Určení jména uživatelského účtu, jehož položky autorun budou zobrazeny.

Tip: Při používaní aplikace Autoruns určené pro příkazový řádek je vhodné výstup vždy přesměrovat do souboru. Prohlížení výpisu několika desítek záznamů může být na obrazovce monitoru komplikovanější. V případě potřeby dalšího (softwarového) zpracování je určitě výhodné použít například formát XML.

Příklad použití Autorunsc.exe

Výpis aplikací a služeb spouštěných po startu operačního systému:

autorunsc

```
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
  Themes Setup
    %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
      %SystemRoot%\system32\themeui.dll
    Windows Theme API
    Microsoft Corporation
    6.1.7601.17514
    c:\windows\system32\themeui.dll
  Microsoft Windows
    "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE
    Windows Mail
    Microsoft Corporation
    6.1.7600.16385
    c:\program files\windows mail\winmail.exe
  [DISABLED] Microsoft Windows Media Player
    %SystemRoot%\system32\unregmp2.exe /ShowWMP
    Microsoft Windows Media Player Setup Utility
    Microsoft Corporation
    12.0.7600.16385
    c:\windows\system32\unregmp2.exe
  [DISABLED] Internet Explorer
    C:\Windows\System32\ie4uinit.exe -UserIconConfig
    IE Per-User Initialization Utility
    Microsoft Corporation
    9.0.8112.16421
    c:\windows\system32\ie4uinit.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  SpybotSD TeaTimer
    C:\Program Files (x86)\Spybot - Search & Destroy\TeaTimer.exe
    System settings protector
    Safer-Networking Ltd.
    1.6.6.32
    c:\program files (x86)\spybot - search & destroy\teatimer.exe
  RESTART_STICKY_NOTES
    C:\Windows\System32\StikyNot.exe
    Rychle poznamky
    Microsoft Corporation
    6.1.7600.16385
    c:\windows\system32\stikynot.exe
  [DISABLED] SymphonyPreLoad
    "C:\Program Files (x86)\IBM\Lotus\Symphony\framework\shared\eclipse\
      plugins\com.ibm.symphony.standard.launcher.win3
      2.x86_3.0.1.20120110-2000\IBM Lotus Symphony" -nogui -nosplash
    IBM
    3.0.0.0
    c:\program files (x86)\ibm\lotus\symphony\framework\shared\eclipse\
```

```
plugins\com.ibm.symphony.standard.launcher.win32
.x86_3.0.1.20120110-2000\ibm lotus symphony.exe
```

Využití

Tento nástroj najde svoje uplatnění zejména ve firemní sféře, kde administrátor může provádět bezpečnostní audit na pracovních stanicích zaměstnanců a kontrolovat tak aplikace, knihovny, služby a další moduly, které se spouštějí po startu systému nebo přihlášení uživatele. Využití není vyloučeno ani v domácím prostředí. Prostřednictvím této utility je možné částečně urychlit start systému, případně přihlášení uživatele, a zkrátit tím čas, za který bude operační systém připraven k použití.

Msconfig

Msconfig je systémová utilita, kterou lze konfigurovat spouštění (bootování) operačního systému, automaticky spouštěné služby a aplikace při startu operačního systému.

Nástroj nabízí pro detailnější nastavení pět karet (viz obrázek 4.5).

Obrázek 4.5 Msconifg

Možnosti nastavení

- **General** – karta, která obsahuje základní nastavení spouštění operačního systému. Vybírat lze ze tří režimů – **Normal**, **Diagnostic**, **Selective**.
- **Boot** – karta umožňující nastavení možnosti multibootu.
- **Services** – na této kartě je možné nastavit spouštění a blokování služeb při startu operačního systému. Obdobné nastavení nabízí i konzole Windows **services.msc**.
- **Startup** – karta obsahuje seznam aplikací, které se spouštějí automaticky po startu operačního systému. V tomto seznamu by mělo být co nejméně aplikací. Velké množství aplikací způsobuje prodlužování doby spouštění operačního systému a doby, kdy bude systém možné používat. Jedinou aplikací, která by se měla v této kategorii každopádně

nacházet na každém systému, je antivirový software, případně ještě softwarový firewall (v případě, že se nevyužívá integrovaný firewall operačního systému).

- **Tools**.

Využití

Msconfig je vhodný při snaze o optimalizaci spouštění operačního systému. Po zakoupení pracovní stanice (osobního počítače, notebooku) s OEM verzí operačního systému bývají v systému taktéž nainstalovány aplikace konkrétního prodejce. Ve většině případů se jedná o aplikace, které běžný uživatel nevyužije, a často jen zbytečně využívají systémové prostředky.

LogonSessions

Název:	LogonSessions	
Velikost:	133 KB	
Kategorie:	Security tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb896769*	

Popis

Nástroj LogonSessions umožňuje zobrazit seznam aktivních uživatelských relací na testovaném systému. Nástroj podporuje jen jeden parametr, který poskytuje výpis rozšířený o seznam procesů spuštěných daným uživatelem.

Příklad použití

V následujícím příkladu bude prezentováno použití nástroje LogonSessions s jediným podporovaným parametrem.

```
logonsessions -p

[0] Logon session 00000000:000003e7:
  User name:    WORKGROUP\VIA-HP$
  Auth package: NTLM
  Logon type:   (none)
  Session:      0
  Sid:          S-1-5-18
  Logon time:   26. 10. 2012 15:05:04
  Logon server:
  DNS Domain:
  UPN:
    276: smss.exe
    428: csrss.exe
    328: svchost.exe
   1040: atieclxx.exe
```

```
   4444: SearchIndexer.exe
   4996: HPWA_Service.exe
   4524: WmiPrvSE.exe
[1] Logon session 00000000:000093d1:
  User name:
  Auth package: NTLM
  Logon type:   (none)
  Session:      0
  Sid:          (none)
  Logon time:   26. 10. 2012 15:05:04
  Logon server:
  DNS Domain:
  UPN:
[2] Logon session 00000000:000003e4:
  User name:    WORKGROUP\VIA-HP$
  Auth package: Negotiate
  Logon type:   Service
  Session:      0
  Sid:          S-1-5-20
  Logon time:   26. 10. 2012 15:05:20
  Logon server:
  DNS Domain:
  UPN:
    828: svchost.exe
   1156: svchost.exe
   1912: sqlservr.exe
   4564: svchost.exe
   4760: wmpnetwk.exe
[3] Logon session 00000000:000003e5:
  User name:    NT AUTHORITY\LOCAL SERVICE
  Auth package: Negotiate
  Logon type:   Service
  Session:      0
  Sid:          S-1-5-19
  Logon time:   26. 10. 2012 15:05:20
  Logon server:
  DNS Domain:
  UPN:
    952: svchost.exe
   2056: svchost.exe
   2276: svchost.exe
[4] Logon session 00000000:0001f3b3:
  User name:    VIA-HP\Tester
  Auth package: NTLM
  Logon type:   Interactive
  Session:      1
  Sid:          S-1-5-21-4172933926-2951322903-2260617033-1001
  Logon time:   26. 10. 2012 15:05:26
  Logon server: VIA-HP
  DNS Domain:
  UPN:
   2384: taskhost.exe
   2556: dwm.exe
```

```
   2588: explorer.exe
   2412: cmd.exe
   1276: conhost.exe
[5] Logon session 00000000:00031be2:
  User name:    NT AUTHORITY\ANONYMOUS LOGON
  Auth package: NTLM
  Logon type:   Network
  Session:      0
  Sid:          S-1-5-7
  Logon time:   26. 10. 2012 15:05:38
  Logon server:
  DNS Domain:
  UPN:
```

Využití

Tento nástroj najde uplatnění hlavně u systémových administrátorů, kteří chtějí mít přehled o aktuálních uživatelských relacích na konkrétním (serverovém) systému.

PsExec

Název:	PsExec	
Velikost:	1,6 MB	
Kategorie:	Security tools	
Typ utility:	CMD	
URL:	*http://technet.microsoft.com/en-us/sysinternals/bb897553*	

Popis

Nástroj je součástí balíku PsTools. PsExec umožňuje vzdálené spouštění procesů na jiných stanicích bez nutnosti instalace klientského softwaru. Utilita byla vytvořena jako alternativa k Telnetu.

Použití

```
psexec [\\computer[,computer2[,...] | @file][-u user [-p psswd]][-n s]
       [-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d]
       [-<priority>][-a n,n,... ] cmd [arguments]
```

Seznam podporovaných parametrů

`computer`	Určení jména vzdálené stanice, na které má nástroj PsExec spouštět aplikace. V případě vynechání tohoto parametru dojde ke spuštění aplikace na lokálním systému. Při použití zástupných znaků `\\*` dojde ke spuštění zadaného příkazu na všech stanicích připojených v aktuální doméně.