100 sposobów na bezpieczeństwo sieci

Autor: Andrew Lockhart
Tłumaczenie: Witold Zioło
ISBN: 83-7361-670-5
Tytuł oryginału: Network Security Hacks
Format: B5, stron: 292

Zbiór porad dla wszystkich, którzy chcą zabezpieczyć swój komputer

- Zainstaluj systemy wykrywania włamań
- Zabezpiecz pocztę elektroniczną
- Ochroń swój system operacyjny

Internet, mimo wielu zalet, niesie za sobą zagrożenie – wielu ludzi wykorzystuje go do działalności niezgodnej z prawem. Każdego dnia krakerzy włamują się do niezabezpieczonych komputerów, zamieniając je w przekaźniki spamu lub wykorzystując jako narzędzia do ataków blokady usług, ukrywając za ich pomocą swoją tożsamość.

„100 sposobów na bezpieczeństwo Sieci" to zbiór porad, dzięki którym zabezpieczysz swój komputer przed atakami sieciowych napastników. Każdy z przykładów został przetestowany w praktyce przez specjalistów zajmujących się na co dzień ochroną danych i systemów. Dzięki nim ochronisz komputer przed najbardziej wyrafinowanymi i przebiegłymi atakami.

- Bezpieczeństwo systemu Windows – poprawki, zabezpieczanie portów i dzienników zdarzeń
- Bezpieczeństwo systemu Unix – zabezpieczanie usług i plików
- Zabezpieczanie Sieci – korzystanie z zapór ogniowych, certyfikatów i szyfrowania
- Rejestrowanie zdarzeń i monitorowanie Sieci
- Metody wykrywania włamań i reagowanie na ataki

„100 sposobów na bezpieczeństwo Sieci" to książka przydatna każdemu użytkownikowi internetu. Dzięki niej, oszczędzając czas, zaimplementujesz sprawdzone i skuteczne mechanizmy zabezpieczeń.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

ROZDZIAŁ DRUGI

Bezpieczeństwo systemu Windows

Sposoby 21. – 30.

W tym rozdziale omówione zostaną niektóre sposoby utrzymania aktualności oraz zabezpieczenia systemu Windows, a tym samym uczynienia ze swojej sieci bezpieczniejszego miejsca do pracy (i zabawy). Mimo że wiele osób uważa użycie w jednym zdaniu wyrazów Windows i bezpieczeństwo za drwinę, to jednak system Windows można całkiem skutecznie zabezpieczyć i to bez większego wysiłku.

Jednym z powodów, dla których system Windows zbiera takie cięgi, jest kiepski stan administracyjny, w którym znajduje się wiele komputerów z tym systemem. Ostatnia plaga robaków i wirusów, która powaliła wiele sieci, świadczy tylko o tym, że w stwierdzeniu tym jest wiele prawdy. Przyczyny tego stanu rzeczy należy szukać w „łatwości" administrowania, jaką zapewnia system Windows, realizowanej przez skuteczne utrzymywanie administratora z dala od tego, co dzieje się wewnątrz systemu, co odbiera administratorowi możliwość panowania nad systemem.

W rozdziale tym szukamy na tę dolegliwość lekarstwa, które przynajmniej w pewnym stopniu pozwoliłoby zobaczyć, co tak naprawdę dzieje się w serwerze. Poznawanie szczegółów otwartych portów oraz działających usług — czynność rutynowa dla doświadczonego administratora systemu Unix — dla wielu przeciętnych administratorów systemu Windows będzie czymś zupełnie nowym. Poza tym rozdział ten przedstawia, jak wyłączyć niektóre „udogodnienia" systemu Windows, takie jak automatyczne udzielanie dostępu do plików czy urywanie dzienników zdarzeń. Można będzie się z niego również dowiedzieć, jak uruchomić w systemie Windows niektóre mechanizmy inspekcji i rejestrowania, które odpowiednio wcześnie powiadomią o wystąpieniu zdarzenia mogącego potencjalnie naruszać bezpieczeństwo systemu (dzięki czemu nie zaskoczy nas telefon od zdenerwowanego administratora sieci, którego dosięgnął właśnie atak blokady usług prowadzony z naszej sieci).

SPOSÓB 21.

Kontrola zainstalowanych poprawek

System Windows powinien mieć zawsze zainstalowane aktualne poprawki[1].

Utrzymanie aktualności systemu Unix jest trudne, ale utrzymanie aktualności systemu Windows może być jeszcze trudniejsze. Brak zaawansowanego, wewnętrznego systemu skryptów oraz możliwości zdalnego dostępu powoduje, że w systemie Windows trudno jest automatyzować jakiekolwiek działania. Poza tym, przed podjęciem próby uaktualnienia systemu, należy się najpierw dowiedzieć, jakie poprawki zostały już zastosowane. W przeciwnym razie można stracić dużo czasu na uaktualnianie systemu, który tego nie wymaga. Oczywiście problem ten przybiera na sile wraz z liczbą zarządzanych systemów. Niepotrzebnego wysiłku ręcznego uaktualniania systemu można uniknąć za pomocą programu *HFNetChk*, który kiedyś był samodzielnym programem oferowanym przez firmę Shavlik Technologies, a teraz jest częścią programu *Microsoft's Baseline Security Analyzer* (*http://www.microsoft.com/downloads/details.aspx?FamilyID=8b7a580d-0c91-45b7-91ba-fc47f7c--3d6ad&DisplayLang=en*), a ściślej został włączony do jego wersji uruchamianej z wiersza poleceń (*mbsacli.exe*).

Program *HFNetChk* nie tylko potrafi zdalnie sprawdzić stan uaktualnień systemów Windows Server 2003 oraz Windows XP/2000/NT, ale również może sprawdzić, czy zainstalowano krytyczne uaktualnienia serwerów IIS, SQL, Exchange, programu *Media Player* oraz przeglądarki *Internet Explorer*. Mimo że program jedynie sprawdza stan uaktualnień systemu (a nie uaktualnia go), i tak jest wartościowym, oszczędzającym czas narzędziem.

Program *HFNetChk* po uruchomieniu pobiera z serwera firmy Microsoft podpisany i skompresowany plik XML, zawierający informacje o aktualnie dostępnych poprawkach. Informacje te zawierają sumy kontrolne oraz numery wersji plików znajdujących się w każdym uaktualnieniu oraz klucze rejestru modyfikowane przez każde uaktualnienie. Dołączona jest również informacja o zależności między uaktualnieniami. Badając system, program *HFNetChk* poszukuje najpierw w rejestrze kluczy najbardziej aktualnych poprawek dostępnych w bieżącej konfiguracji systemu operacyjnego. Jeżeli w systemie brakuje jakiegoś klucza rejestru lub wartość tego klucza nie odpowiada informacji zapisanej w pliku XML, program traktuje takie uaktualnienie jako niezainstalowane. Jeżeli w rejestrze znajduje się klucz poprawki odpowiadający informacjom z pliku XML, program *HFNetChk* sprawdza, czy pliki wymienione w informacji o uaktualnieniu są w systemie obecnie i czy ich wersje i sumy kontrolne są odpowiednie. Jeżeli któreś z tych sprawdzeń zakończy się niepowodzeniem, program traktuje takie uaktualnienie jako niezainstalowane. Wszystkie niezainstalowane uaktualnienia są wymieniane w tworzonym raporcie, łącznie z odniesieniem do odpowiedniego artykułu Bazy Wiedzy, zawierającym bardziej szczegółowe informacje o danym uaktualnieniu.

[1] W terminologii systemu Windows termin „łatka" został zastąpiony terminem „poprawka". Można się z tym zgodzić, szczególnie, że natura oraz sposób stosowania łatek i poprawek jest zupełnie inny — *przyp. tłum.*

Aby zainstalować program *HFNetChk*, należy najpierw pobrać i zainstalować program *Microsoft Baseline Security Analyzer*[2]. Aby uruchomić program, należy otworzyć wiersz polecenia i przejść do katalogu, w którym zainstalowany został *Microsoft Baseline Security Analyzer*. Domyślnie jest to katalog *C:\Program Files\Microsoft Baseline Security Analyzer*.

Aby zbadać stan uaktualnień lokalnego systemu, należy wydać następujące polecenie:

```
C:\> Program Files\Microsoft Baseline Security Analyzer> mbsacli /hf
Microsoft Baseline Security Analyzer
Version 1.1.1
Powered by HFNetChk Technology - Version 3.82.0.1
Copyright (C) Shavlik Technologies, 2001-2003
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)


Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages


Attempting to get cab from http://go.microsoft.com/fwlink/?LinkId=16932


XML successfully loaded.


Scanning PLUNDER
.........................
Done scanning PLUNDER
---------------------------
PLUNDER(192.168.0.65)
---------------------------

        * WINDOWS XP SP1

        Note            MS02-008        317244
        Warning         MS02-055        323255
        Note            MS03-008        814078
        Note            MS03-030        819696
        Patch NOT Found MS03-041        823182
        Patch NOT Found MS03-044        825119
        Patch NOT Found MS03-045        824141
        Patch NOT Found MS03-049        828035
        Note            MS03-051        813360

        * INTERNET EXPLORER 6 SP1

        Patch NOT Found MS03-048        824145

        * WINDOWS MEDIA PLAYER FOR WINDOWS XP SP1

        Information
        All necessary hotfixes have been applied.
```

[2] Program *HFNetChk* w dalszym ciągu pozostaje samodzielną aplikacją, a pobrać go można po zarejestrowaniu się na stronie *http://www.shavlik.com/pDownloadForm4.aspx — przyp. tłum.*

Pierwsza kolumna informuje, dlaczego sprawdzenie obecności uaktualnienia nie powiodło się. Druga kolumna określa, którego uaktualnienia to dotyczy, a trzecia zawiera numer artykułu Bazy Wiedzy (*http://support.microsoft.com*), zawierającego więcej informacji na temat problemu rozwiązywanego przez dane uaktualnienie.

Jeżeli sprawdzenie obecności którejś poprawki zakończyło się niepowodzeniem, za pomocą opcji `-v` można uzyskać więcej informacji o przyczynie tego niepowodzenia. Oto wyniki działania poprzedniego polecenia, użytego tym razem dodatkowo z opcją `-v`:

```
Scanning PLUNDER
.........................
Done scanning PLUNDER
---------------------------
PLUNDER(192.168.0.65)
---------------------------

        * WINDOWS XP SP1

        Note            MS02-008        317244
        Please refer to Q306460 for a detailed explanation.

        Warning         MS02-055        323255
        File C:\WINDOWS\system32\hhctrl.ocx has a file
        version [5.2.3735.0] greater than what is expected [5.2.3669.0].

        Note            MS03-008        814078
        Please refer to Q306460 for a detailed explanation.

        Note            MS03-030        819696
        Please refer to Q306460 for a detailed explanation.

        Patch NOT Found MS03-041        823182
        File C:\WINDOWS\system32\cryptui.dll has a file
        version [5.131.2600.1106] that is less than what is expected
        [5.131.2600.1243].

        Patch NOT Found MS03-044        825119
        File C:\WINDOWS\system32\itircl.dll has a file
        version [5.2.3644.0] that is less than what is expected
        [5.2.3790.80].

        Patch NOT Found MS03-045        824141
        File C:\WINDOWS\system32\user32.dll has a file
        version [5.1.2600.1134] that is less than what is expected
        [5.1.2600.1255].

        Patch NOT Found MS03-049        828035
        File C:\WINDOWS\system32\msgsvc.dll has a file
        version [5.1.2600.0] that is less than what is expected
        [5.1.2600.1309].

        Note            MS03-051        813360
        Please refer to Q306460 for a detailed explanation.


        * INTERNET EXPLORER 6 SP1

        Patch NOT Found MS03-048        824145
        The registry key **SOFTWARE\Microsoft\Internet Explorer\ActiveX
```

```
Compatibility\{69DEAF94-AF66-11D3-BEC0-00105AA9B6AE}** does not
exist.  It is required for this patch to be considered installed.


* WINDOWS MEDIA PLAYER FOR WINDOWS XP SP1

Information
All necessary hotfixes have been applied.
```

Po zastosowaniu brakujących poprawek wynik działania programu wygląda następująco:

```
Scanning PLUNDER
.........................
Done scanning PLUNDER
---------------------------
PLUNDER(192.168.0.65)
---------------------------

        * WINDOWS XP SP1

        Information
        All necessary hotfixes have been applied.

        * INTERNET EXPLORER 6 SP1

        Information
        All necessary hotfixes have been applied.

        * WINDOWS MEDIA PLAYER FOR WINDOWS XP SP1

        Information
        All necessary hotfixes have been applied.
```

Do zbadania stanu uaktualnień w systemie potrzebne są uprawnienia administratora. Jeżeli zbadany ma być stan uaktualnień komputera zdalnego, potrzebne będą uprawnienia administratora w jego systemie. Istnieje kilka sposobów zbadania stanu uaktualnień komputerów zdalnych. Aby zbadać pojedynczy komputer, można w opcji `-h` podać jego nazwę NetBIOS. Aby zamiast tego móc posłużyć się adresem IP, należy użyć opcji `-i`.

Aby na przykład zbadać zdalnie komputer PLUNDER, można posłużyć się jednym z dwóch poleceń:

```
mbsacli /hf -h PLUNDER
mbsacli /hf -i 192.168.0.65
```

Można też przebadać kilka systemów jeden po drugim, podając w wierszu poleceń ich nazwy NetBIOS lub adresy IP, oddzielone od siebie przecinkami.

Należy pamiętać, że poza posiadaniem uprawnień administratora do systemu zdalnego, w systemie tym nie może być wyłączony udział domyślny **[Sposób 27.]**, w przeciwnym razie program *HFNetChk* nie będzie w stanie stwierdzić obecności odpowiednich plików w jego systemie, a w konsekwencji nie będzie mógł sprawdzić, czy uaktualnienie zostało zastosowane.

Istnieje również kilka możliwości zbadania całej grupy systemów. Za pomocą opcji `-fh` można podać nazwę pliku zawierającego do 256 nazw NetBIOS komputerów (każda nazwa w osobnym wierszu), które mają zostać przebadane. Podobnie, za pomocą opcji `-fip` można podać ich adresy IP. Za pomocą opcji `-r` można określać zakresy adresów IP.

Aby na przykład zbadać systemy o adresach IP w zakresie od 192.168.1.123 do 192.168.1.172, należy wydać polecenie:

```
mbsacli /hf -r 192.168.1.123 - 192.168.1.172
```

Wszystkie opisane tu opcje są bardzo elastyczne i można używać ich kombinacji.

Poza podawaniem nazwy NetBIOS albo adresu IP, można również za pomocą opcji `-d` podać nazwę domeny lub za pomocą opcji `-n` zbadać cały lokalny segment sieci.

Przy badaniu systemów zdalnych ze stacji roboczej przydatne mogą okazać się opcje `-u` i `-p`. Umożliwiają one podanie nazwy użytkownika oraz hasła, potrzebnych do uzyskania dostępu do zdalnego systemu. Opcje te są szczególnie przydatne, gdy nie logujemy się na konto Administratora. Oczywiście użytkownik określony za pomocą opcji `-u` musi posiadać w zdalnym systemie uprawnienia administracyjne.

W przypadku badania dużej liczby systemów, warto posłużyć się opcją `-t`. Określa ona liczbę wątków używanych przez program, a zwiększenie tej liczby na ogół przyśpiesza badanie. Dopuszczalnymi wartościami są liczby z przedziału od 1 do 128. Wartością domyślną jest liczba 64.

W przypadku badania więcej niż jednego komputera, na ekranie pojawi się wiele danych. Za pomocą opcji `-f` można podać nazwę pliku, do którego zostaną zapisane wyniki badania i który można będzie przejrzeć w późniejszym czasie za pomocą edytora tekstu.

Program *HFNetChk* jest niezwykle elastycznym narzędziem i może być używany do badania stanu uaktualnień dużej liczby komputerów, i to w dość krótkim czasie. Szczególnie przydatny bywa wówczas, gdy na horyzoncie pojawia się nowy robak i trzeba bardzo szybko sprawdzić, czy wszystkie systemy mają zainstalowane aktualne poprawki.

Zobacz również

- Microsoft Network Security Hotfix Checker (*Hfnetchk.exe*) — artykuł w Bazie Wiedzy o numerze 303215, dostępny pod adresem *http://support.microsoft.com/default.aspx?scid=kb;en-us;303215*
- Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (*Hfnetchk.exe*) artykuł w Bazie Wiedzy o numerze 305385, dostępny pod adresem *http://support.microsoft.com/default.aspx?scid=kb;en-us;305385*

SPOSÓB 22.

Lista otwartych plików oraz procesów, które ich używają

Monitorując korzystanie z plików, można wykryć podejrzaną aktywność.

Wyobraźmy sobie, że po zauważeniu dziwnego zachowania stacji roboczej, przyglądając się liście procesów Menedżera zadań, dostrzegliśmy tam nazwę nieznanego procesu. Co w takim przypadku można zrobić? W przypadku innego systemu operacyjnego można by stwierdzić, co robi ten proces, sprawdzając, jakie pliki otworzył. Niestety w systemie Windows nie ma odpowiedniego do tego celu narzędzia.

Firma Sysinternals stworzyła[3] znakomite narzędzie o nazwie *Handle*, dostępne za darmo pod adresem *http://www.sysinternals.com/ntw2k/freeware/handle.shtml*. Program *Handle* bardzo przypomina program *lsof* **[Sposób 8.]**, z tym że informuje również o wielu innych zasobach systemu operacyjnego takich jak wątki, zdarzenia czy semafory. Pokazuje także otwarte klucze rejestru oraz struktury IOCompletion.

Program *Handle*, uruchomiony bez dodatkowych parametrów, pokazuje uchwyty wszystkich otwartych w systemie plików. Po podaniu jako parametru nazwy pliku, program pokaże listę procesów korzystających aktualnie z tego pliku:

```
C:\> handle nazwa_pliku
```

Można też uzyskać listę plików otwartych przez określony proces, w poniższym przykładzie — przez przeglądarkę *Internet Explorer*:

```
C:\> handle -p iexplore
Handle v2.10
Copyright (C) 1997-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

------------------------------------------------------------------------------
IEXPLORE.EXE pid: 688 PLUNDER\andrew
   98: Section       \BaseNamedObjects\MTXCOMM_MEMORY_MAPPED_FILE
   9c: Section       \BaseNamedObjects\MtxWndList
  12c: Section       \BaseNamedObjects\__R_0000000000d4_SMem_ _
  18c: File          C:\Documents and Settings\andrew\Local Settings\
Temporary Internet Files\Content.IE5\index.dat
  198: Section       \BaseNamedObjects\C:_Documents and Settings_andrew_
Local Settings_Temporary Internet Files_Content.IE5_index.dat_3194880
  1a0: File          C:\Documents and Settings\andrew\Cookies\index.dat
  1a8: File          C:\Documents and Settings\andrew\Local Settings\
History\History.IE5\index.dat
  1ac: Section       \BaseNamedObjects\C:_Documents and Settings_andrew_
Local Settings_History_History.IE5_index.dat_245760
  1b8: Section       \BaseNamedObjects\C:_Documents and Settings_andrew_
Cookies_index.dat_81920
  228: Section       \BaseNamedObjects\UrlZonesSM_andrew
  2a4: Section       \BaseNamedObjects\SENS Information Cache
  540: File          C:\Documents and Settings\andrew\Application Data\
Microsoft\SystemCertificates\My
```

[3] Firma ta jest autorem wielu innych prawdziwych pereł darmowego oprogramowania systemowego, między innymi programów *TCPView*, *Process Explorer*, *File Monitor* czy *Registry monitor* — *przyp. tłum.*

```
  574: File          C:\Documents and Settings\All Users\Desktop
  5b4: Section       \BaseNamedObjects\mmGlobalPnpInfo
  5cc: File          C:\WINNT\system32\mshtml.tlb
  614: Section       \BaseNamedObjects\WDMAUD_Callbacks
  640: File          C:\WINNT\system32\Macromed\Flash\Flash.ocx
  648: File          C:\WINNT\system32\STDOLE2.TLB
  6a4: File          \Dfs
  6b4: File          C:\Documents and Settings\andrew\Desktop
  6c8: File          C:\Documents and Settings\andrew\Local Settings\
Temporary Internet Files\Content.IE5\Q5USFST0\softwareDownloadIndex[1].htm
  70c: Section       \BaseNamedObjects\MSIMGSIZECacheMap
  758: File          C:\WINNT\system32\iepeers.dll
  75c: File          C:\Documents and Settings\andrew\Desktop
  770: Section       \BaseNamedObjects\RotHintTable
```

Chcąc odnaleźć proces *Internet Explorera* korzystający z zasobu, którego nazwa zawiera wyraz „handle", należy użyć następującego polecenia:

```
C:\> handle -p iexplore handle
Handle v2.10
Copyright (C) 1997-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

IEXPLORE.EXE       pid: 1396   C:\Documents and Settings\andrew\
Local Settings\Temporary
Internet Files\Content.IE5\H1EZGFSH\handle[1].htm
```

Chcąc obejrzeć listę wszystkich zasobów, należy posłużyć się opcją `-a`. Program *Handle* jest bardzo wszechstronnym narzędziem, umożliwiającym użycie naraz kilku opcji wiersza poleceń, dzięki czemu szybko można odnaleźć poszukiwany element.

SPOSÓB 23.

Lista działających usług i otwartych portów

Kontrola dostępnych zdalnie usług systemu Windows.

W Uniksie można bardzo szybko sprawdzić, które porty systemu są otwarte, ale jak to zrobić w systemie Windows[4]? Z pomocą przychodzi, podobny do starego dobrego programu *netstat*, program *FPort* firmy Foundstone (*http://www.foundstone.com/resources/index_resources.htm*).

Program *FPort* ma niewiele opcji wiersza poleceń, a dostępne opcje decydują głównie o sposobie sortowania prezentowanych informacji. Jeżeli na przykład informacje należy posortować według nazw programów, należy użyć opcji `/a`, a jeżeli według identyfikatorów procesu — opcji `/i`. I choć program nie ma tylu funkcji co *netstat*, niewątpliwie to co robi, robi dobrze.

Aby uzyskać listę otwartych w systemie portów, wystarczy wydać polecenie `fport`. Jeżeli lista ta ma być posortowana według numeru portu, należy dodatkowo użyć opcji `/p`:

[4] Można to zrobić, o czym autor najwyraźniej zapomniał, za pomocą tego samego co w systemie Unix — programu *netstat*, dostępnego we wszystkich systemach Windows, a w systemach Windows XP/2000/2003 informującego dodatkowo o identyfikatorach procesów używających portów — *przyp. tłum*.

```
C:\> fport /p
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
432   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
672   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
8     System         ->  1028  TCP
8     System         ->  1031  TCP
1116  navapw32       ->  1035  TCP   C:\PROGRA~1\NORTON~1\navapw32.exe
788   svchost        ->  1551  TCP   C:\WINNT\system32\svchost.exe
788   svchost        ->  1553  TCP   C:\WINNT\system32\svchost.exe
788   svchost        ->  1558  TCP   C:\WINNT\system32\svchost.exe
1328  svchost        ->  1565  TCP   C:\WINNT\System32\svchost.exe
8     System         ->  1860  TCP
1580  putty          ->  3134  TCP   C:\WINNT\putty.exe
772   WinVNC         ->  5800  TCP   C:\Program Files\TightVNC\WinVNC.exe
772   WinVNC         ->  5900  TCP   C:\Program Files\TightVNC\WinVNC.exe

432   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
256   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
244   services       ->  1027  UDP   C:\WINNT\system32\services.exe
688   IEXPLORE       ->  2204  UDP   C:\Program Files\Internet Explorer\
IEXPLORE.EXE
1396  IEXPLORE       ->  3104  UDP   C:\Program Files\Internet Explorer\
IEXPLORE.EXE
256   lsass          ->  4500  UDP   C:\WINNT\system32\lsass.exe
```

Należy zauważyć, że niektóre wymienione procesy, takie jak *navapw32*, *putty* oraz *IEXPLORE*, nie są procesami. Ich nazwy pojawiły się na ekranie, gdyż *FPort* przedstawia informacje o wszystkich otwartych portach, nie tylko o portach nasłuchujących.

I mimo że program *FPort* nie ma tylu możliwości co programy dostępne w innych systemach operacyjnych, jest wartościowym, działającym szybko i łatwym w użyciu narzędziem, znakomicie uzupełniającym system Windows.

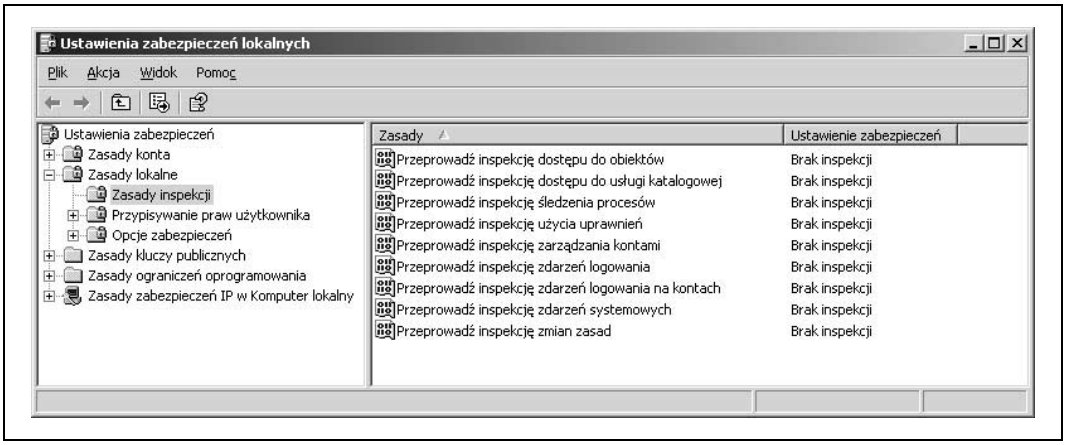
SPOSÓB 24.

Uruchomienie inspekcji

Rejestrowanie podejrzanej aktywności pomaga w wykryciu intruzów.

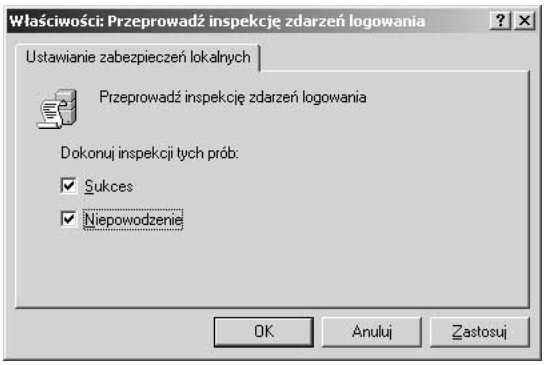
System Windows 2000 wyposażono w bardzo efektywną funkcję inspekcji, niestety domyślnie jest ona wyłączona. W systemie Windows 2003 naprawiono to, uaktywniając domyślnie kilka jej funkcji, mimo to warto sprawdzić, czy inspekcji podlega to co trzeba. Na przykład istnieje możliwość monitorowania zakończonego niepowodzeniem logowania, zdarzeń związanych z zarządzaniem kontami, dostępu do plików, użycia uprawnień i wielu innych zdarzeń. Można również rejestrować zmiany polityki bezpieczeństwa oraz zdarzenia systemowe.

Aby włączyć inspekcję w jednej z tych kategorii, należy kliknąć dwukrotnie znajdującą się w *Panelu sterowania* ikonę *Narzędzia administracyjne*, następnie ikonę *Zasady zabezpieczeń lokalnych* i rozwinąć węzeł *Zasady lokalne*. Na ekranie powinien pojawić się widok podobny do pokazanego na rysunku 2.1.



Rysunek 2.1. Ustawienia zasad inspekcji w aplecie Ustawienia zabezpieczeń lokalnych

Teraz można zapoznać się z każdą zasadą inspekcji i zdecydować, czy rejestrować powodzenia, czy niepowodzenia każdej z nich. W tym celu należy dwukrotnie kliknąć modyfikowaną zasadę znajdującą się w prawej części okna, po czym na ekranie pojawi się okno dialogowe podobne do przedstawionego na rysunku 2.2.



Rysunek 2.2. Okno dialogowe Przeprowadź inspekcję zdarzeń logowania

Niewłączanie inspekcji jest równoważne z nierejestrowaniem niczego, dlatego należy włączyć inspekcję wszystkich zasad. Po włączeniu inspekcji określonej zasady w dziennikach zdarzeń zaczną pojawiać się pozycje informujące o sukcesach i niepowodzeniach zdarzeń tej zasady. Na przykład po włączeniu rejestracji zdarzeń logowania, w dzienniku zdarzeń Zabezpieczenia pojawiać się będą komunikaty informujące o powodzeniu lub niepowodzeniu logowania.

SPOSÓB 25.

Zabezpieczenie dzienników zdarzeń

Systemowe dzienniki zdarzeń należy chronić przed modyfikacją.

System Windows wyposażony jest w bardzo zaawansowane funkcje rejestracji zdarzeń. Niestety, domyślnie dzienniki zdarzeń nie są chronione przed nieautoryzowanym dostępem ani przed modyfikacją. Przeglądając dzienniki za pomocą programu *Podgląd zdarzeń*, można nie być świadomym tego, że przechowywane są w zwykłych plikach. Zatem, aby je zabezpieczyć, wystarczy je odnaleźć, a następnie utworzyć dla nich poprawne listy ACL.

O ile położenie dzienników zdarzeń nie zostało zmienione w rejestrze, można je znaleźć w katalogu *%SystemRoot%\system32\config*.

Znajdują się tam trzy pliki: *AppEvent.Evt*, *SecEvent.Evt* i *SysEvent.Evt*, odpowiadające kolejno Dziennikowi aplikacji, Dziennikowi zabezpieczeń i Dziennikowi systemu. Dla plików tych należy utworzyć listy ACL, umożliwiające korzystanie z nich jedynie administratorowi. W tym celu należy w oknie *Właściwości* plików wybrać zakładkę *Zabezpieczenia*, a następnie usunąć z górnego panelu wszystkich użytkowników i grupy poza Administratorzy i SYSTEM.

SPOSÓB 26.

Zmiana maksymalnej wielkości dzienników zdarzeń

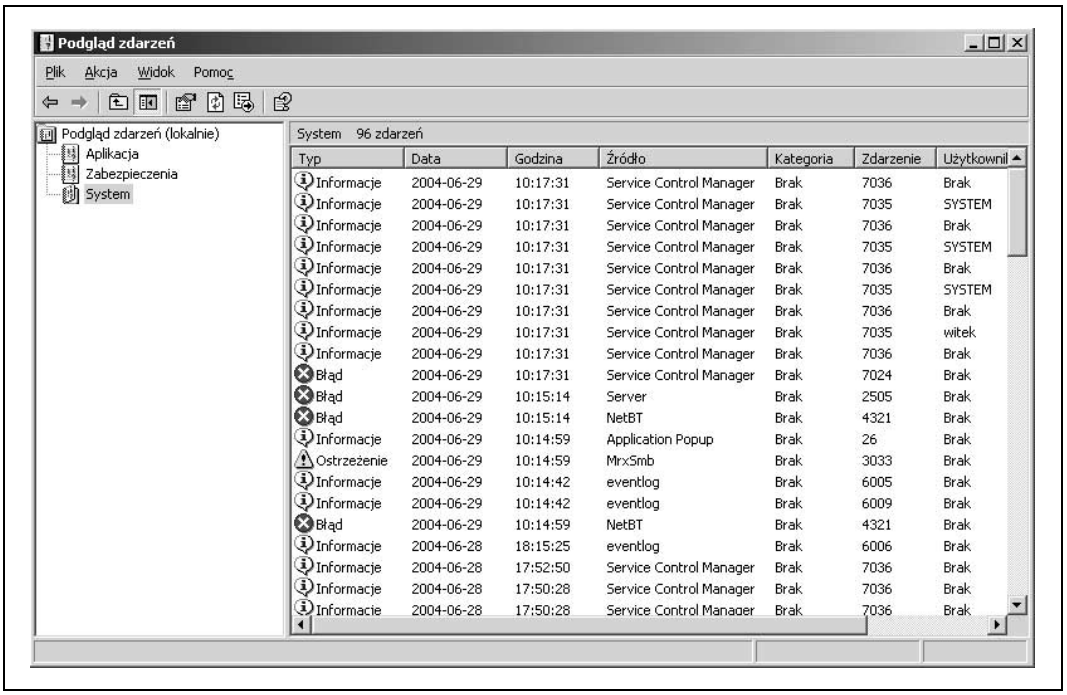
Żeby dzienniki zdarzeń zawierały cały obraz wydarzeń, należy zmienić niektóre ich właściwości.

Z punktu widzenia bezpieczeństwa dzienniki zdarzeń są jednym z najbardziej wartościowych zasobów serwera. Bez nich nie byłoby możliwości stwierdzenia, czy i kiedy ktoś wdarł się do komputera. Dlatego absolutną koniecznością jest, by dzienniki niczego nie przeoczyły. W przypadku śledzenia incydentu naruszenia bezpieczeństwa, brak jakiś zapisów w dzienniku zdarzeń ma taki sam skutek jak brak dzienników w ogóle.

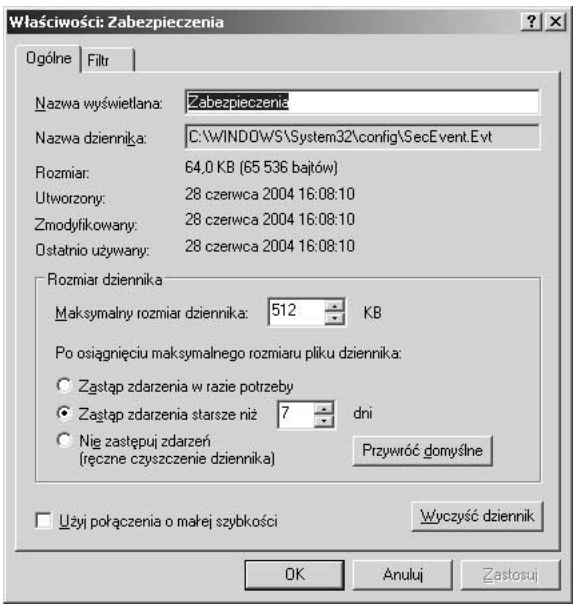
Często występującym problemem jest zbyt mała maksymalna wielkość plików dzienników zdarzeń, wynosząca domyślnie zaledwie 512 KB. Aby to zmienić, należy w panelu *Narzędzia administracyjne* uruchomić program *Podgląd zdarzeń*. Na ekranie pojawi się widok pokazany na rysunku 2.3.

W lewym panelu okna *Podgląd zdarzeń* należy wybrać jeden z dzienników zdarzeń, kliknąć go prawym przyciskiem myszy, a następnie wybrać *Właściwości*. Pojawi się okno dialogowe pokazane na rysunku 2.4.

W oknie należy odnaleźć pole tekstowe *Maksymalny rozmiar dziennika*. Nową wartość maksymalnej wielkości pliku dziennika można wpisać w pole bezpośrednio lub ustalić za pomocą znajdujących się obok pola strzałek. Wprowadzona wartość powinna być nie mniejsza niż 1 MB, a zależy ona od tego, jak często dzienniki są przeglądane i archiwizowane. Warto pamiętać, że zwiększenie wielkości plików dzienników zdarzeń nie spowoduje zwiększenia obciążenia serwera, a jedynie może to mieć wpływ na szybkość ich przeglądania za pomocą programu *Podgląd zdarzeń*. W tym samym oknie dialogowym można również zmienić zachowanie dzienników zdarzeń po osiągnięciu przez nie maksymalnej wielkości. Domyślnie w takim przypadku zapisy starsze niż siedmiodniowe są



Rysunek 2.3. Podgląd zdarzeń systemu Windows



Rysunek 2.4. Właściwości dziennika zabezpieczeń

nadpisywane. Zaleca się zwiększenie tej wartość na przykład do 31 dni. Można również nie zezwolić na automatyczne nadpisywanie dzienników zdarzeń — w takim przypadku trzeba je będzie czyścić ręcznie.

SPOSÓB 27.

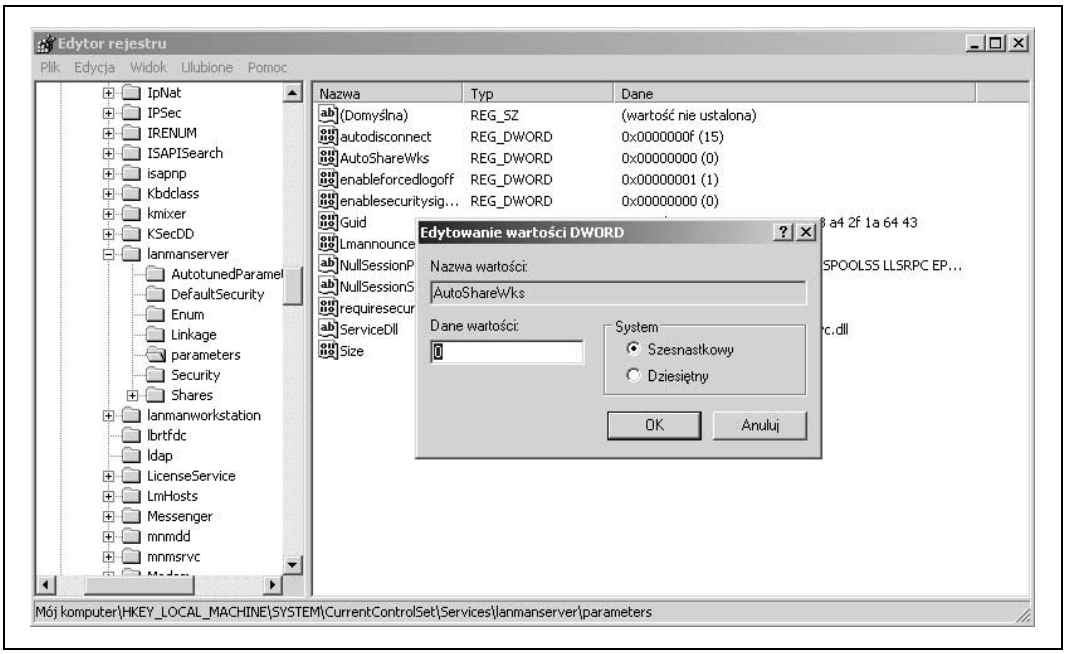
Wyłączenie udziałów domyślnych

Czyli jak przestać udostępniać swoje pliki całemu światu.

System Windows tworzy udział domyślny dla każdego dysku logicznego (na przykład *C$* dla dysku C) oraz dodatkowo dla katalogu *%SystemRoot%* (czyli na przykład *C:\WINNT*) tworzy udział o nazwie *ADMIN$*. Mimo że dostępne one są jedynie dla administratorów, warto je jednak wyłączyć (jeżeli to możliwe), gdyż stanowią potencjalną lukę w bezpieczeństwie.

Aby wyłączyć udziały domyślne, należy za pomocą programu *regedit.exe* otworzyć rejestr do edycji, a następnie odszukać w nim klucz `HKey_Local_Machine\SYSTEM\Current➥ControlSet\Services\lanmanserver\parameters`.

W przypadku stacji roboczej z systemem Windows 2000 należy dodać do klucza wartość DWORD `AutoShareWks` o danej równej `0` (co pokazano na rysunku 2.5). W tym celu należy wybrać *Edycja/Nowy/ Wartość DWORD*. W przypadku serwera Windows 2000 należy dodać wartość `AutoShareServer` również o danej równej `0`. Aby zmiany wprowadzone do rejestru odniosły skutek, system Windows należy uruchomić ponownie.



Rysunek 2.5. Dodawanie do rejestru wartości AutoShareWks

Aby upewnić się, że domyślny udział już nie istnieje, należy po ponownym uruchomieniu systemu Windows wydać polecenie `net share`:

```
C:\>net share

Udział       Zasób                        Uwaga

-------------------------------------------------------------------------------
IPC$                                      Zdalne wywołanie IPC
Polecenie zostało wykonane pomyślnie.
```

Przed wyłączeniem udziałów domyślnych należy upewnić się, że nie wpłynie to negatywnie na środowisko sieciowe. Brak dostępu do udziałów może spowodować, że niektóre programy (takie jak *HFNetChk* **[Sposób 21.]** czy System Management Server) nie będą działać. Dzieje się tak dlatego, że programy tego typu wykorzystują udziały administracyjne do uzyskania dostępu do zawartości dysków.

SPOSÓB 28.

Zaszyfrowanie folderu Temp

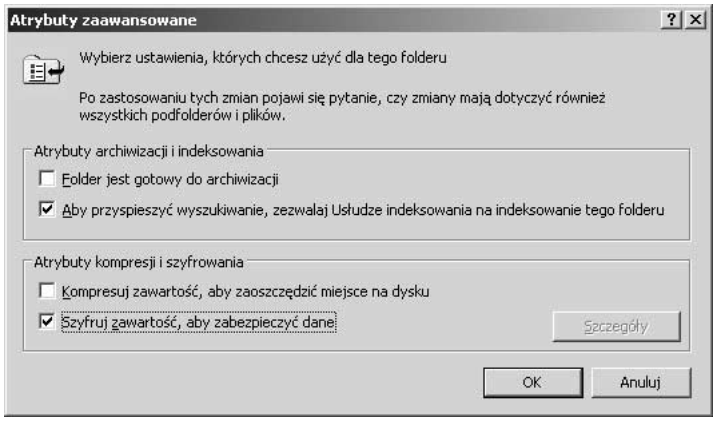
Przed wścibskimi oczami trzeba chronić również pliki tymczasowe.

Wiele programów systemu Windows tworzy podczas pracy pliki tymczasowe. Programy umieszczają je przeważnie w specjalnie przeznaczonym do tego celu folderze, znajdującym się w katalogu bieżącego użytkownika. Wiele z tych plików jest dostępnych do odczytu dla wszystkich, a nie zawsze są one usuwane po zakończeniu działania programu. Świadomość, że na przykład edytor tekstu pozostawił tam kopię ostatnio tworzonego dokumentu nie należy do przyjemnych. Nieprawdaż?

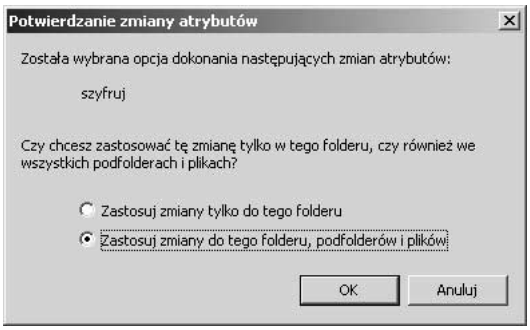
Jednym ze sposobów zabezpieczenia się przed tego typu niespodziankami jest zaszyfrowanie folderu plików tymczasowych. W tym celu należy uruchomić program *Explorator Windows* i przejść w nim do folderu *C:\Documents and Settings\<nazwa_użytkownika>\Ustawienia lokalne*. W folderze tym znajduje się folder *Temp*, przechowujący pliki tymczasowe. Po kliknięciu go prawym przyciskiem myszy i wybraniu pozycji *Właściwości* należy wybrać zakładkę *Ogólne* i nacisnąć przycisk *Zaawansowane*. Na ekranie pojawi się pokazane na rysunku 2.6 okno dialogowe *Atrybuty zaawansowane*, w którym można polecić zaszyfrowanie folderu.

Następnie należy zaznaczyć pole wyboru *Szyfruj zawartość, aby zabezpieczyć dane* i nacisnąć przycisk *OK*. Po powrocie do okna *Właściwości* należy nacisnąć przycisk *Zastosuj*. Pojawi się okno dialogowe pokazane na rysunku 2.7, zawierające pytanie, czy zaszyfrowane mają zostać również podfoldery wybranego folderu.

Aby zaszyfrowane zostały również podfoldery, należy wybrać opcję *Zastosuj zmiany do tego folderu, podfolderów i plików*. Jeżeli żadne foldery w systemie nie były jeszcze nigdy szyfrowane, utworzona zostanie para kluczy. W przeciwnym razie system użyje klucza publicznego utworzonego wcześniej. Podczas odszyfrowywania, system Windows przechowuje klucze prywatne w niestronicowanej pamięci jądra, zatem nie ma niebezpieczeństwa, że zostaną one zapisane w pliku stronicowania. Niestety, zastosowany do szyfrowania algorytm DESX jest tylko nieznacznym usprawnieniem algorytmu DES i nie jest



Rysunek 2.6. Okno dialogowe Atrybuty zaawansowane katalogu Temp



Rysunek 2.7. Potwierdzenie szyfrowania folderu i jego podfolderów

tak bezpieczny jak 3DES. Mimo to do szyfrowania plików tymczasowych zupełnie wystarczy. Do szyfrowania innych plików niż tymczasowe lepiej jest użyć programów twórców niezależnych, na przykład *GnuPG* (*http://www.gnupg.org*), dostępnego również dla systemu Windows.

SPOSÓB 29.

Czyszczenie pliku stronicowania podczas zamykania systemu

Aby zapobiec wyciekaniu informacji, system przed zatrzymaniem powinien automatycznie wyczyścić zawartość pliku stronicowania.

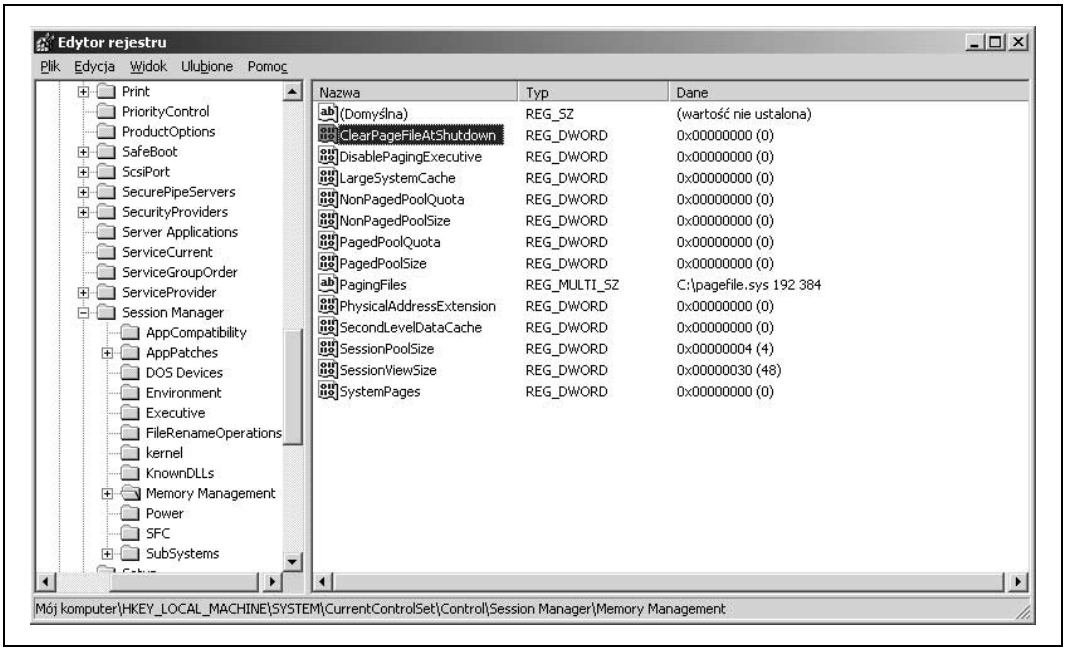
Mechanizm zarządzania pamięcią wirtualną (VMM) jest znakomitym rozwiązaniem. Chroni on programy jeden przed drugim i powoduje, że uważają one, iż dysponują większą ilością pamięci niż pamięć fizycznie zainstalowana w systemie. Do tego celu mechanizm VMM wykorzystuje tak zwany *plik stronicowania*.

Po uruchomieniu kilku programów w systemie może zabraknąć wolnej pamięci fizycznej. Ponieważ nie można do tego dopuścić, menedżer pamięci szuka najrzadziej używanego fragmentu pamięci należącego do programu, który w danej chwili akurat nic nie robi i zapisuje ten obszar pamięci na dysk. Proces ten nazywany jest *wymianą*.

Mechanizm ten ma jednak jedną wadę. Jeżeli jakiś program przechowuje w pamięci informacje poufne, zawartość tej strony pamięci może zostać zapisana na dysk. Kiedy system operacyjny pracuje, niczym to nie grozi, gdyż system zabezpiecza plik stronicowania przed odczytem. Gorzej jest, gdy system zostanie wyłączony lub w komputerze zostanie uruchomiony inny system operacyjny.

W tym miejscu z pomocą przychodzi ta porada. Powiemy w niej, jak nakazać systemowi operacyjnemu, by w momencie jego zamykania wypełnił plik stronicowania zerami. Należy jednak pamiętać, że rozwiązanie to na nic się nie zda, gdy ktoś wyjmie wtyczkę z gniazdka zasilającego lub system zostanie zatrzymany w sposób nieprawidłowy. Sposób ten działa jedynie wówczas, gdy system jest zamykany prawidłowo.

Aby uruchomić tę funkcję systemu Windows, należy dokonać zmian w rejestrze. W tym celu należy uruchomić edytor rejestru i otworzyć klucz `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`. Na ekranie pojawi się widok pokazany na rysunku 2.8.



Rysunek 2.8. Klucz rejestru Memory Management

W prawym panelu okna należy odnaleźć wartość `ClearPageFileAtShutdown` i zmienić jej daną na `1`. Aby wprowadzona zmiana odniosła skutek, system należy uruchomić ponownie. Od tej pory podczas każdego zamykania systemu plik wymiany będzie czysz-

czony. Jedyną wadą uruchomienia tego mechanizmu jest wydłużenie czasu trwania procesu zamykania systemu. Jednak ile czasu będzie trwało nadpisane pliku stronicowania zerami, zależy od używanego sprzętu (układów scalonych kontrolera dysku, szybkości dysku, szybkości procesora i tym podobnych).

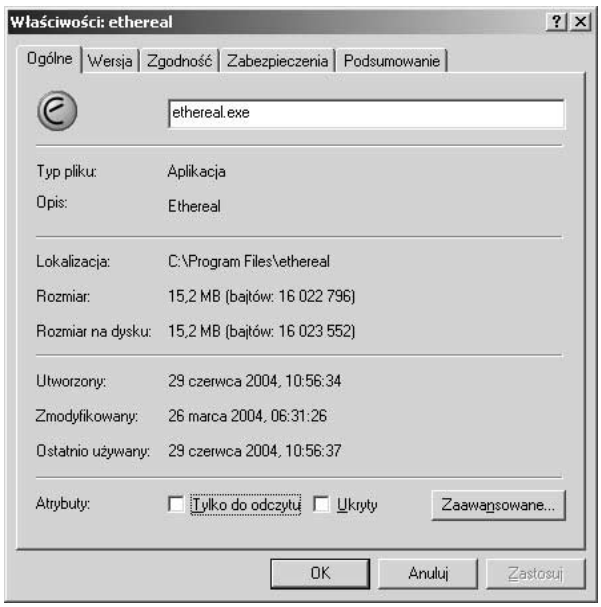
SPOSÓB 30.

Ograniczenie aplikacji dostępnych użytkownikom

Warto uniemożliwić użytkownikom uruchamianie potencjalnie niebezpiecznych programów.

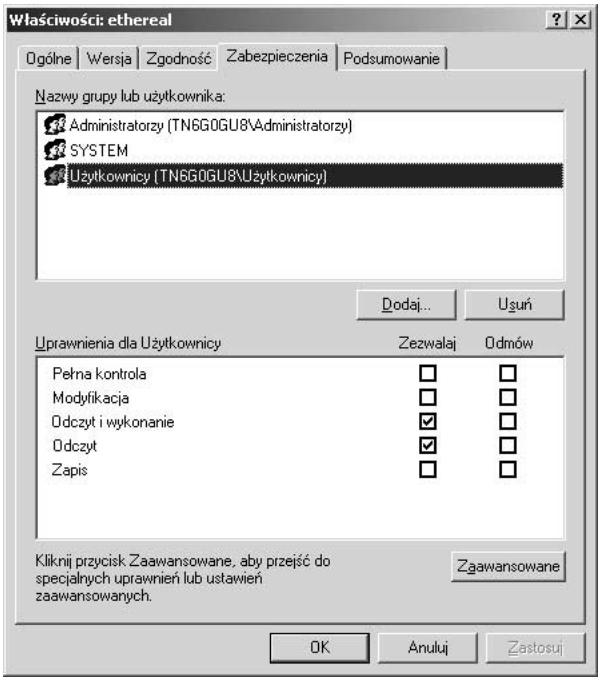
Uniemożliwianie użytkownikom uruchamiania pewnych aplikacji nie ma takiego znaczenia, gdy administrator przechowuje wszystkie programy administracyjne w swojej stacji roboczej. W przypadku użytkowników dużych środowisk sieciowych nie można pozwolić, by mogli oni używać szkodliwych programów. Należą do nich programy, które mogą zniszczyć system operacyjny, utworzyć luki w bezpieczeństwie systemu, a nawet atakować inne komputery w sieci.

Istnieje kilka sposobów ograniczania aplikacji dostępnych dla użytkownika. Pierwszy z nich polega na modyfikacji listy ACL danego programu, tak by nie mogli go używać zwykli użytkownicy. Załóżmy na przykład, że w systemie użytkownika zainstalowany został do celów diagnostycznych szperacz (ang. *sniffer*). Korzystać z tego rodzaju programów powinien móc jedynie administrator, ale nie zwykli użytkownicy. Aby uniemożliwić im uruchamianie programu, należy odebrać grupie Użytkownicy uprawnienia do wykonywania programu. W tym celu należy znaleźć plik wykonywalny programu, kliknąć go prawym przyciskiem myszy i z menu podręcznego wybrać pozycję *Właściwości*. Na ekranie pojawi się okno dialogowe pokazane na rysunku 2.9.



Rysunek 2.9. Okna dialogowe Właściwości pliku ethereal.exe — szperacza Ethereal

Następnie należy kliknąć zakładkę *Zabezpieczenia* i z listy znajdującej się w górnej części okna wybrać grupę *Użytkownicy*. Na ekranie pojawi się widok pokazany na rysunku 2.10.

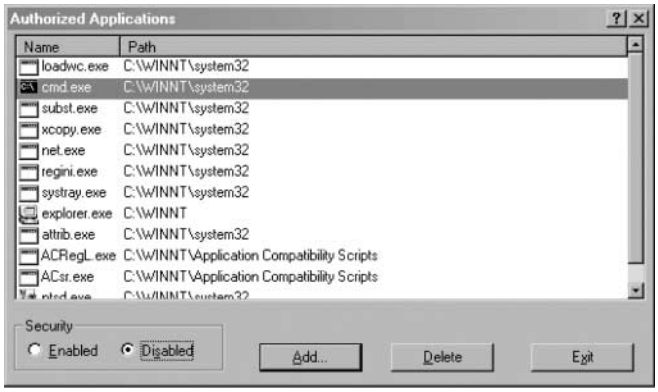


Rysunek 2.10. Zakładka Zabezpieczenia okna dialogowego Właściwości pliku ethereal.exe

Teraz w pozycji uprawnień *Odczyt i wykonywanie* należy zaznaczyć pole *Odmów*. Po naciśnięciu przycisku *Zastosuj* żaden z członków grupy Użytkownicy nie będzie mógł uruchomić programu. Można by również zmienić listę ACL katalogu, w którym znajduje się program i zabronić odczytu z niego. To rozwiązanie jest lepsze, gdy wszystkie narzędzia administracyjne są przechowywane w jednym folderze i można w ten sposób za jednym razem ograniczyć korzystanie z nich wszystkich.

W przypadku wersji terminalowej systemu Windows istnieje inna możliwość poza użyciem list ACL. W pakiecie Microsoft Windows 2000 Resource Kit znajduje się program *AppSec*, umożliwiający zabronienie użycia wybranego programu za pomocą kilku kliknięć. Po odnalezieniu i uruchomieniu, program *AppSec* przedstawi listę programów. Jeżeli program, którego wykonywania należy zabronić użytkownikom korzystającym z terminali, znajduje się na liście, wystarczy wybrać opcję *Disabled*. Aby na przykład zabronić użycia programu *cmd.exe*, należy postąpić tak, jak pokazano na rysunku 2.11.

Jeżeli programu, do którego dostęp ma być ograniczony, nie ma na liście, należy nacisnąć przycisk *Add*, a następnie odnaleźć go na dysku. Aby zakończyć działanie programu, należy nacisnąć przycisk *Exit*. Żeby wprowadzone zmiany odniosły skutek, wszyscy użytkownicy muszą się wylogować z serwera terminali.



Rysunek 2.11. Ograniczenie uruchamiania programu cmd.exe