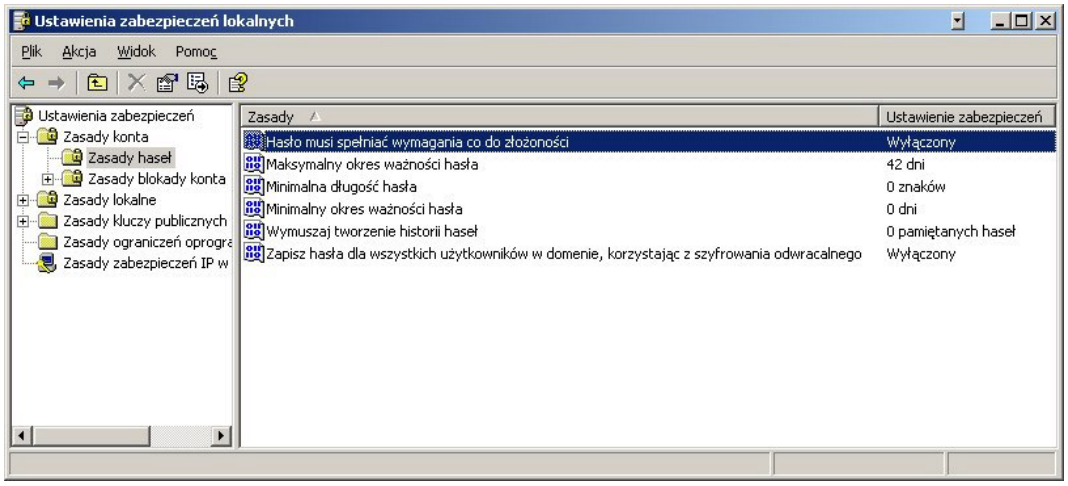
Umacnianie ochrony systemu operacyjnego MS Windows

1 Wprowadzenie

Systemy operacyjne w rodziny Microsoft Windows należą niewątpliwie do liderów popularności na rynku systemów operacyjnych. W większości zastosować domowych popularne Windowsy sprawdzają się bardzo dobrze, co owocuje dużym przywiązaniem użytkowników do tych produktów. Istnieją zastosowania w których systemy te słabo bądź w ogóle nie sprawdzają się jednakże z powodu wygody użytkowania i przystępnego środowiska graficznego są liderem na rynku systemów biurkowych. Systemy MS Windows posiadają wbudowane mechanizmy podwyższające bezpieczeństwo i znajomość tych podstawowych rozwiązań powinna być znana każdemu użytkownikowi tych systemów. W niniejszym opracowaniu zostaną przedstawione różne aspekty odnośnie podnoszenia poziomu bezpieczeństwa pracy w systemach MS Windows XP. Rozwiązania prezentowane należą do grupy zabiegów określanych mianem utwardzania systemu(*ang. system hardening*) i mają na celu podnieść poziom bezpieczeństwa oferowanego przez system. Posługując się określeniem system Windows autor ma na myśli system Microsoft Windows XP Professional z dodatkiem SP2.

2 Konta użytkowników

Pierwszą czynnością podczas pracy z systemem Windows XP jest zalogowanie się do systemu. W większości przypadków konto na które następuje logowanie jest chronione hasłem użytkownika. Możliwe jest również automatyczne logowanie na konto danego użytkownika bez podawania hasła. Jednak taka konfiguracja jest niezalecana. System Windows posiada rozbudowane możliwości konfiguracji różnych aspektów odnośnie kont użytkowników i procedury logowania. Opcje konfiguracyjne zlokalizowane są w oknie `Ustawienia zabezpieczeń lokalnych` i podgrupach `Zasady konta` i `Zasady haseł`. Poniżej zaprezentowano zrzut ekranowy prezentujący okno ustawień zabezpieczeń lokalnych:



Rysunek 1 Okno Ustawień zabezpieczeń lokalnych.

Zadania:

1. Zweryfikuj trudność złamania haseł w systemie za pomocą wybranego narzędzia typu reactive password checking(np. LC4).
2. Włącz opcję `hasło ma spełniać wymagania co do złożoności` i ustaw następujące parametry:

   - `maksymalny wiek hasła: 42 dni`
   - `minimalna długość hasła: 8 znaków`
   - `minimalny okres ważności hasła: 2 dni`
   - `24 ostatnie hasła pamiętane w historii`
   - `wyłączone odwracalne szyfrowanie haseł`

3. Ustaw następujące parametry `blokady konta:`

   - `próg blokady: 4 próby`
   - `czas trwania blokady: 30 minut`
   - `zerowanie licznika prób: po 30 minutach`

4. Wyłącz przechowywanie skrótów kryptograficznych haseł w postaci LMhash:

   - Znajdź odpowiednią opcję(Zasady zabezpieczeń lokalnych, grupa Opcje zabezpieczeń, atrybut: „Zabezpieczenia sieci: nie przechowuj wartości hash programu LAN Manager).
   - Sprawdź ponownie programem LC4 czy skróty Lmhash są dostępne.

2.1 Inspekcja zdarzeń logowania

Inspekcję(ang. Logging) zdarzeń logowania można włączyć poprzez `Ustawienia zabezpieczeń lokalnych`. Inspekcja ta jest jednym z elementów `Zasad lokalnych`. Zarejestrowane zdarzenia można przeglądać przy pomocy programu `Podgląd zdarzeń` w

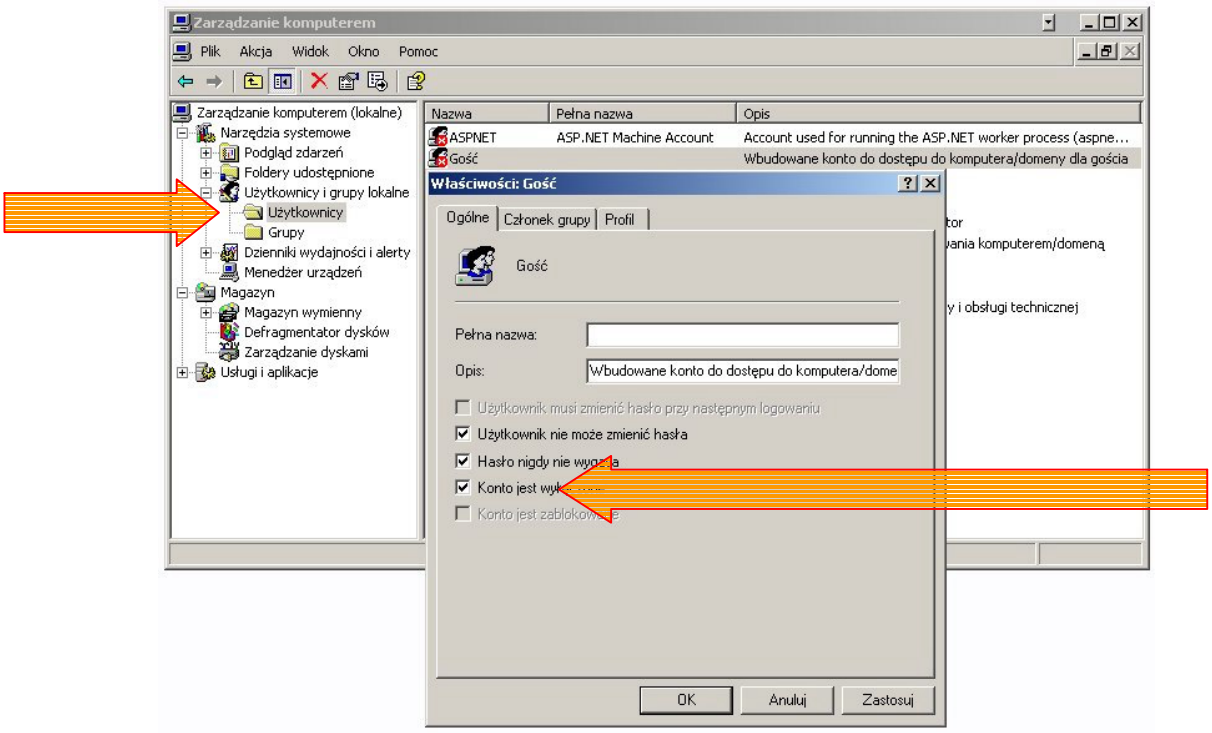
pozycji `System`.

Zadania:

- Włącz i przetestuj inspekcję zdarzeń logowania zakończonych sukcesami i niepowodzeniem.

2.2 Dezaktywacja kont

Wszelkie konta (w tym szczególnie konta zakładane domyślnie przez system lub aplikacje) poza rzeczywiście niezbędnymi powinny być zablokowane (lub usunięte). Poniżej zaprezentowano okno konsoli zarządzania komputerem z uaktywnionym podglądem właściwości dla użytkownika „Gość”:



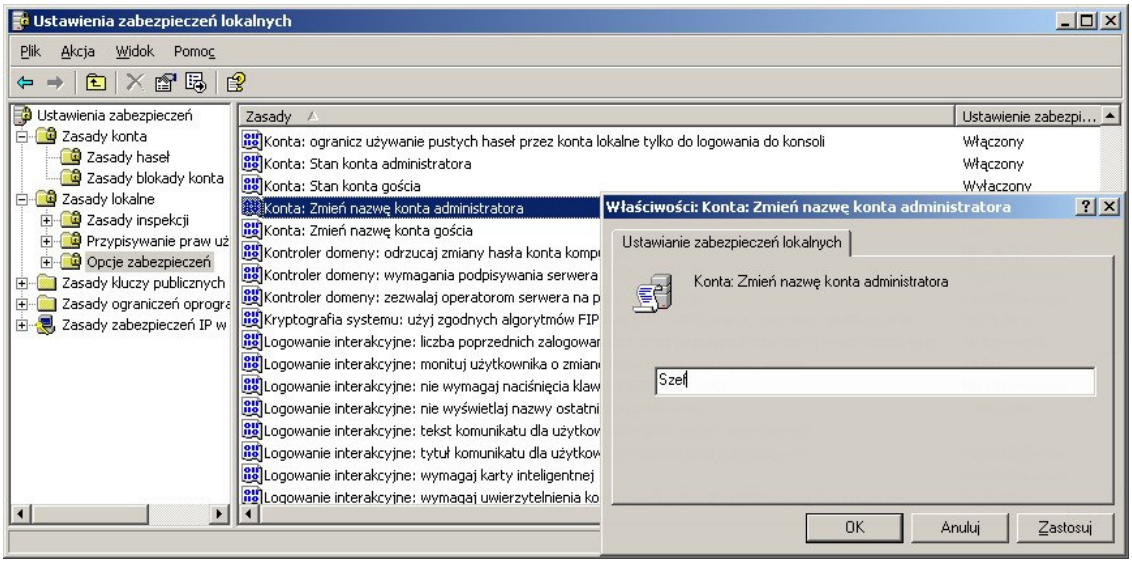
Rysunek 2 Okno konsoli zarządzania komputerem z uaktywnionym podglądem właściwości dla użytkownika „Gość”.

Zadania:

- Zidentyfikuj i wyłącz nieużywane konta.

2.3 Konta użytkowników uprzywilejowanych

Konta użytkowników uprzywilejowanych należy szczególnie starannie chronić przed wykorzystaniem przez osoby nieuprawnione. W pewnym stopniu można utrudnić nielegalne wykorzystanie konta Administratora (włamanie) poprzez zmianę standardowej nazwy tego konta, często oczekiwanej przez intruzów. Jednak wszelkie konta w systemie posiadają oprócz nazw także identyfikatory numeryczne, które nie ulegają zmianie nawet po ewentualnej zmianie nazwy konta (zaawansowane metody ataku korzystają z takich identyfikatorów). Poniżej zaprezentowano zrzut ekranowy pokazując w jaki sposób można zmienić nazwę użytkownika uprzywilejowanego:



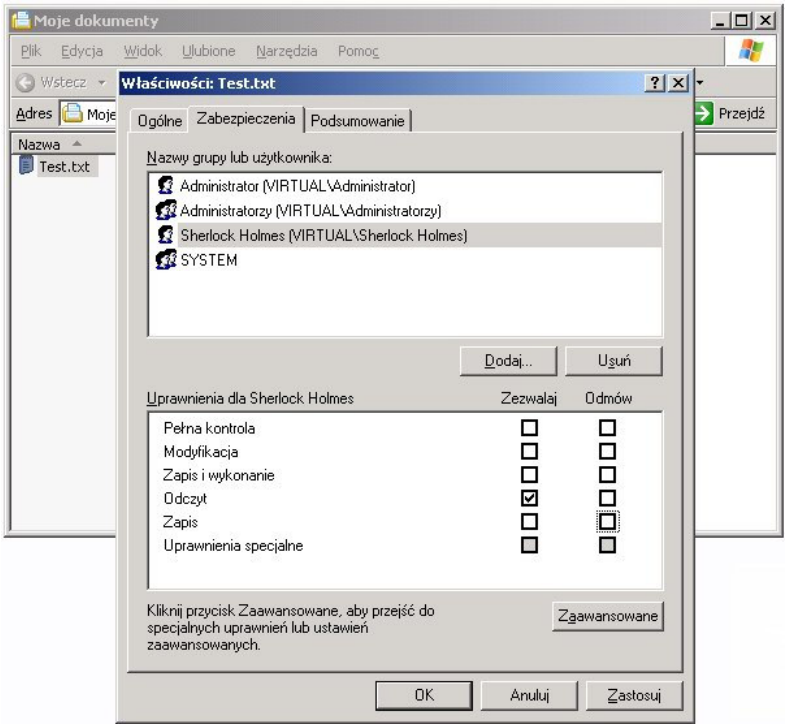
Rysunek 3 Zmiana nazwy konta użytkownika uprzywilejowanego.

Zadania:

- Zmień nazwę konta Administratora. Zweryfikuj zdalnie (np. za pomocą narzędzia `wininfo`) dostępne informacje o kontach w swoim systemie.

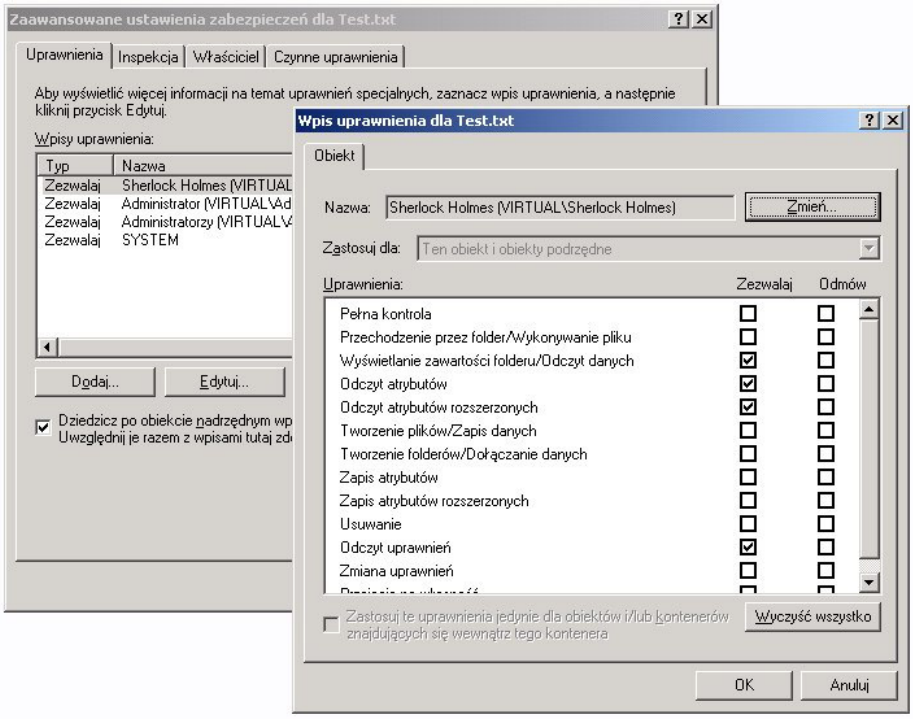
3 System plików

System plików NTFS umożliwia związanie z każdym zasobem plikowym (w tym: katalogiem) list kontroli dostępu ACL (*Access Control List*). Dostęp do prostych ustawień ACL pliku (katalogu) jest możliwy z poziomu np. Eksploratora Windows w opcji Właściwości (menu Plik lub kontekstowe). Poniżej zaprezentowano okno właściwości dla wybranego pliku:



Rysunek 4 Okno właściwości dla wybranego pliku.

Rozszerzone listy ACL są dostępne po wyborze uprawnień zaawansowanych:



Rysunek 5 Rozszerzone listy ACL są dostępne po wyborze uprawnień zaawansowanych

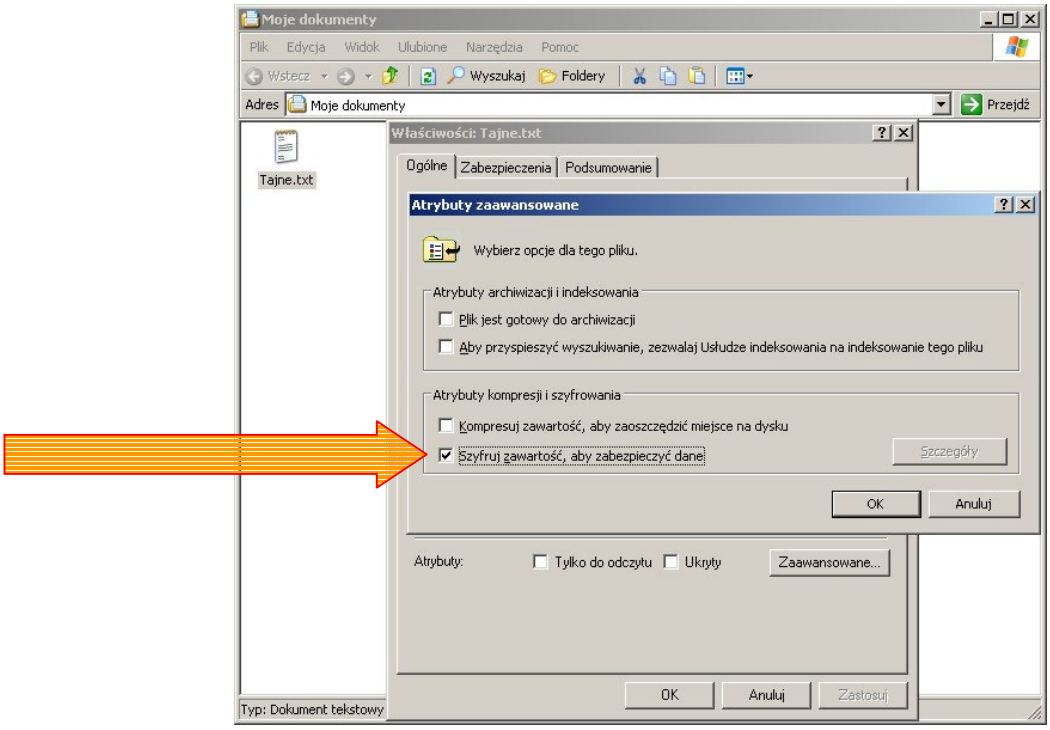
Zadania:

- Zaloguj się na konto administratora (Szef).
- Utwórz w katalogu `Moje dokumenty` plik `Test.txt`. Dla tego pliku wykonaj następujące operacje:
    - korzystając z prostych ACL nadaj uprawnienia do odczytu dla użytkownika Sherlock Holmes
    - sprawdź rozszerzone ACL dla tego użytkownika
    - sprawdź jakie czynne uprawnienia posiada ten użytkownik.

- Następnie dla pliku `Test.txt`:
    - sprawdź jakie czynne uprawnienia posiada użytkownik James Bond
    - korzystając z prostych ACL odbierz uprawnienia do zapisu użytkownikowi James Bond
    - sprawdź rozszerzone ACL dla tego użytkownika
    - sprawdź jakie czynne uprawnienia posiada ten użytkownik.

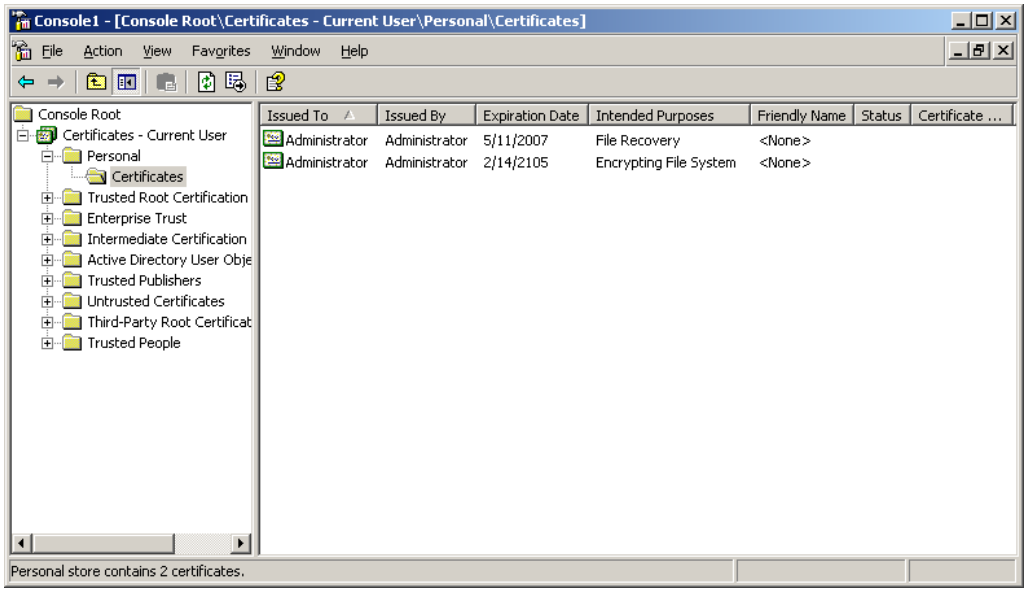
3.1 Szyfrowanie danych

System plików NTFS umożliwia również ochronę kryptograficzną zasobów plikowych, metodą szyfrowania symetrycznego (algorytmem DESX). Poniżej zaprezentowano zrzut ekranowy z oknem właściwości dotyczących szyfrowania:



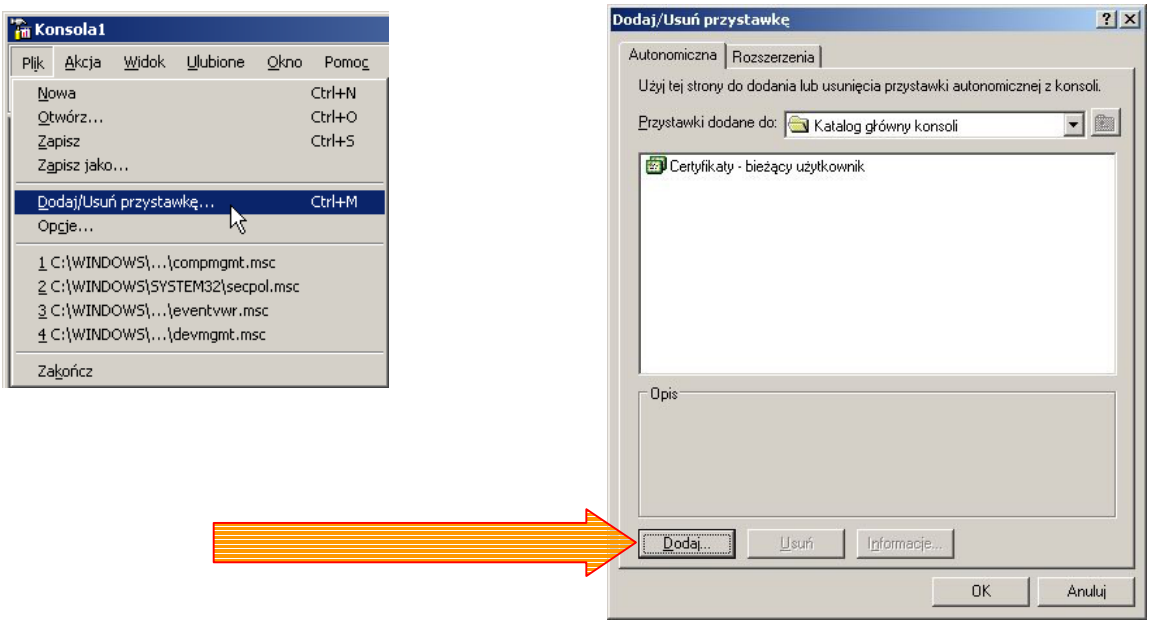
Rysunek 6 Okno właściwości pliku odnośnie szyfrowania.

Użyty do szyfrowania klucz właściciela pliku przechowywany jest w certyfikacie użytkownika. Razem z nim system operacyjny utrzymuje też klucz uniwersalny usługi systemowej `Data Recovery Agent`. Klucze te są widoczne w aplikacji Microsoft Management Console (program mmc). Poniżej zaprezentowano okno konsoli zarządzania certyfikatami:



Rysunek 7 Okno konsoli zarządzania certyfikatami.

Po uruchomieniu konsoli należy z menu Plik wybrać opcję Dodaj/Usuń przystawkę (np. klawiszem ^M), a następnie dodać przystawkę `Certyfikaty – bieżą użytkownik`:



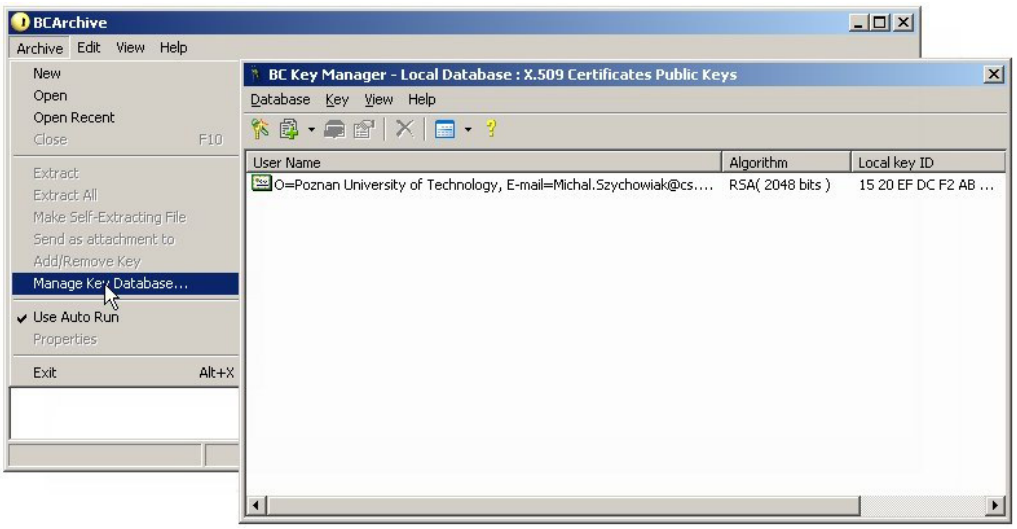
Rysunek 8 Dodanie przystawki: Certyfikaty – bieżący uzytkownik.

Zadania:

- Utwórz plik tekstowy `Tajne.txt` o dowolnej treści. Wyświetl jego zawartość w Eksploratorze oraz w konsoli tekstowej (np. poleceniem `type`).
- Następnie zaszyfruj ten plik i spróbuj ponownie wyświetlić jego zawartość.
- Wyświetl informacje o zaszyfrowanym pliku poleceniem `efsinfo`.
- Odszukaj certyfikat EFS klucza szyfrowania.
- Zaloguj się jako inny użytkownik i spróbuj wyświetlić zawartość tego pliku.

3.2 Archiwa z ochroną kryptograficzną

Wiele programów kompresujących i archiwizujących posiada możliwość zabezpieczania spakowanych danych hasłem dostępu. Wśród takich produktów wyróżnia się BCarchive (firmy Jetico) oferujący profesjonalną ochronę kryptograficzną z wykorzystaniem szyfrowania asymetrycznego i certyfikatami kluczy publicznych. Umożliwia to bezpieczny dostęp do zawartości archiwum np. odbiorcy pocztowemu bez potrzeby uprzedniego ustalania hasła lub klucza. Poniżej zaprezentowano okno programu BCarchive:

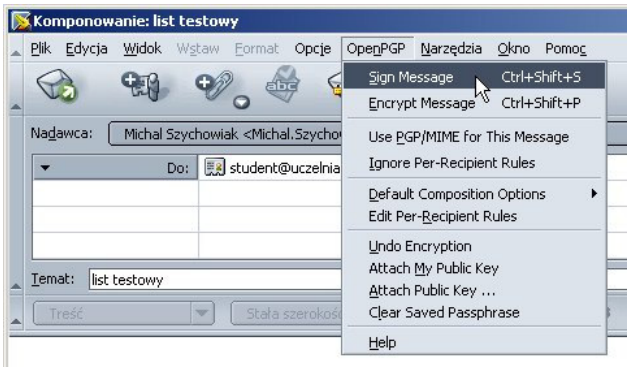


Rysunek 9 Okno programu BCarchive.

4 Poczta elektroniczna

Niektóre programy klientów posiadają możliwość wykorzystania mechanizmów kryptograficznych: szyfrowania i / lub podpisywania korespondencji pocztowej. Taką możliwość posiadają np. popularne produkty z rodziny Mozilla (Mozilla Mail lub Thunderbird) z rozszerzeniem Enigmail (na platformę Windows to rozszerzenie trzeba zainstalować oddzielnie). Enigmail integruje klienta pocztowego z popularnym i powszechnie stosowanym w Internecie systemem PGP (np. pakiet OpenPGP lub GnuPG, niezależnie instalowane w systemie). System PGP umożliwia m.in. certyfikację kluczy pocztowych metodą wzajemnego zaufania (*Web of Trust*). Poniżej zaprezentowano okno klienta poczty Mozilla Mail

zintegrowanego z dodatkiem Enigmail:



Rysunek 10 Klient poczty zintegrowany z dodatkiem Enigmail.

Zadania:

- Zainstaluj system GnuPG oraz rozszerzenie Enigmail klienta pocztowego Mozilla Thunderbird.
- Korzystając w programie Thunderbird z funkcji OpenPGP→Key Management wygeneruj swoją parę kluczy kryptograficznych.
- Wyślij podpisany list do siebie samego. Sprawdź reakcję systemu.
- Wyślij podpisany list do innego użytkownika ze swojej grupy i odbierz jego list.
- Zweryfikuj poprawność podpisu otrzymanego listu.
- Zrealizuj komunikację z szyfrowaniem całej przesyłki pocztowej

4.1 Certyfikaty adresów pocztowych

Jednym z bardziej popularnych ośrodków certyfikacji w Internecie jest firma Thawte. Wiele przeglądarek WWW i aplikacji pocztowych zawiera certyfikat głównego urzędu certyfikacji tej firmy, co pozwala ufać podpisom tego urzędu. Poniżej zaprezentowano certyfikat firmy Thawte:

Rysunek 11 Certyfikat cyfrowy.

Korzystając ze strony http://www.thawte.com można pozyskać darmowy certyfikat poświadczający własny adres pocztowy:

Rysunek 12 Strona www firmy Thawte.

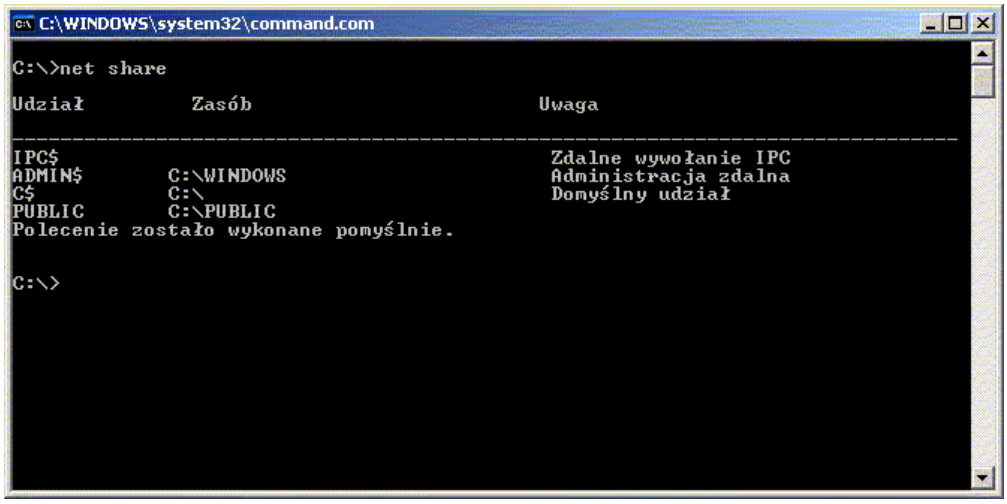
5 Środowisko sieciowe

Rdzennymi w środowisku MS Windows protokołami sieciowymi obsługującymi zasoby

udostępniane w otoczeniu sieciowym są NetBIOS i SMB (*Server Message Block*). Nie są to, niestety, wyrafinowane protokoły, szczególnie pod względem bezpieczeństwa.

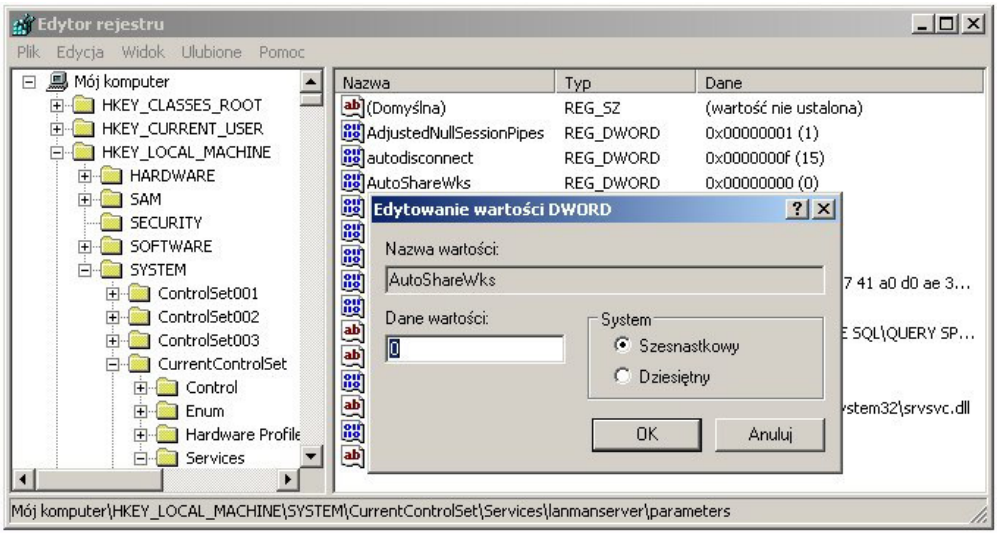
5.1 Otoczenie sieciowe i udziały sieciowe

Udziałami nazywa się w protokole SMB udostępnione poprzez sieć zasoby systemu operacyjnego. Polecenie `net` z argumentem `share` pozwala wyświetlić listę udziałów bieżącego systemu:



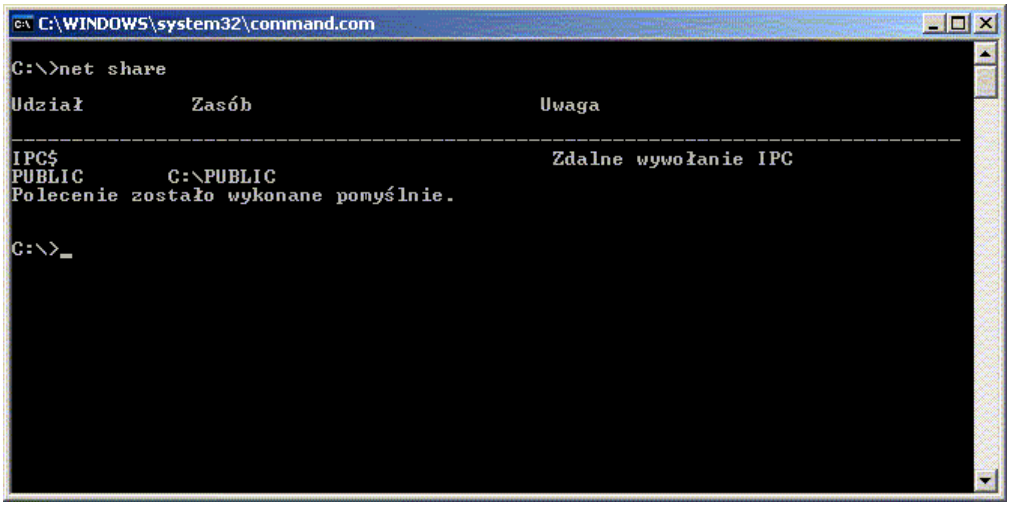
Rysunek 13 Lista udostępnionych zasobów.

Systemy MS Windows bezpośrednio po instalacji tworzą pewne udziały domyślne (dla Windows XP są to np. `C$` oraz `ADMIN$`), które, jakkolwiek na ogół nie stanowią istotnej luki bezpieczeństwa, często nie są potrzebne i powinny być wyłączone. W tym celu niezbędna jest modyfikacja rejestru systemowego. Dla systemu Windows XP w gałęzi `HLM\SYSTEM\CurrentControlSet\Services\LanManServer` w kluczu `parameters` należy dodać wartość `AutoShareWks` typu DWORD równą 0:



Rysunek 14 Modyfikacja rejestru systemowego.

Po załadowaniu tak zmodyfikowanego rejestru (po restarcie) udziały domyślne nie są widoczne:



Rysunek 15 Okno terminala tekstowego wyświetlające udostępnione udziały sieciowe.

Zadania:

- Usuń udziały domyślne swojego stanowiska komputerowego. Zweryfikuj rezultat.

5.2 Ukrycie komputera w otoczeniu sieciowym

W systemie Windows XP istnieje możliwość ukrycia nazwy bieżącego komputera w otoczeniu sieciowym, z zachowaniem jednocześnie możliwości udostępniania zasobów. Ukrycie takie w

czasie bieżącej sesji umożliwia polecenia `net` z argumentem `config server`:

```
C:\> net config server /hidden:yes
```

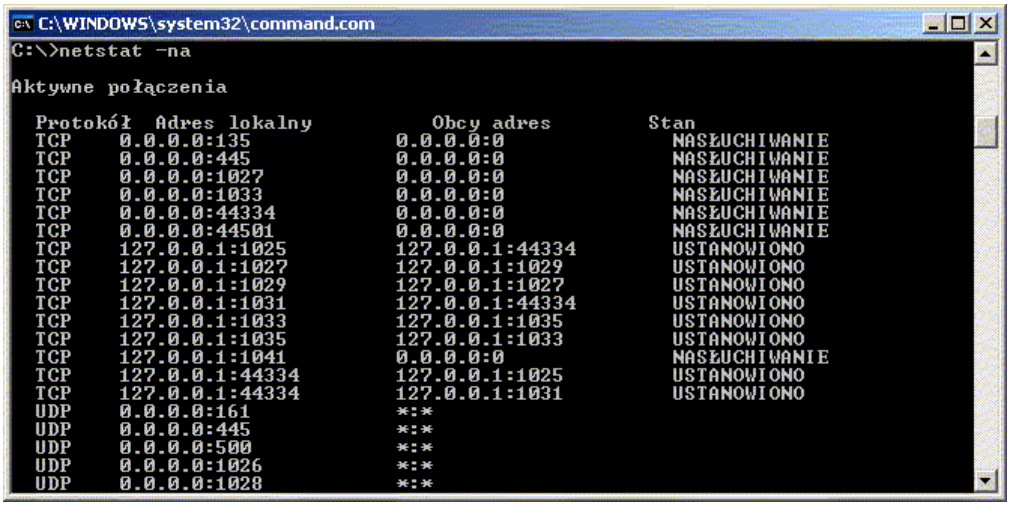
`/hidden` – opcja ukrycia nazwy w otoczeniu sieciowym, możliwe wartości `yes` oraz `no`
Aby trwale uczynić nazwę bieżącego komputera niewidoczną w otoczeniu sieciowym należy zmodyfikować wpis w rejestrze systemowym w gałęzi
HLM\SYSTEM\CurrentControlSet\Services\LanManServer
w kluczu `parameters` należy dodać wartość `Hidden` typu DWORD równą 1.

Zadania:

- Sprawdź widoczność swojego stanowiska w otoczeniu sieciowym. Przetestuj ukrywanie jego nazwy. Czy cały czas możliwe jest korzystanie z udostępnianych zasobów?

5.3 Połączenia sieciowe

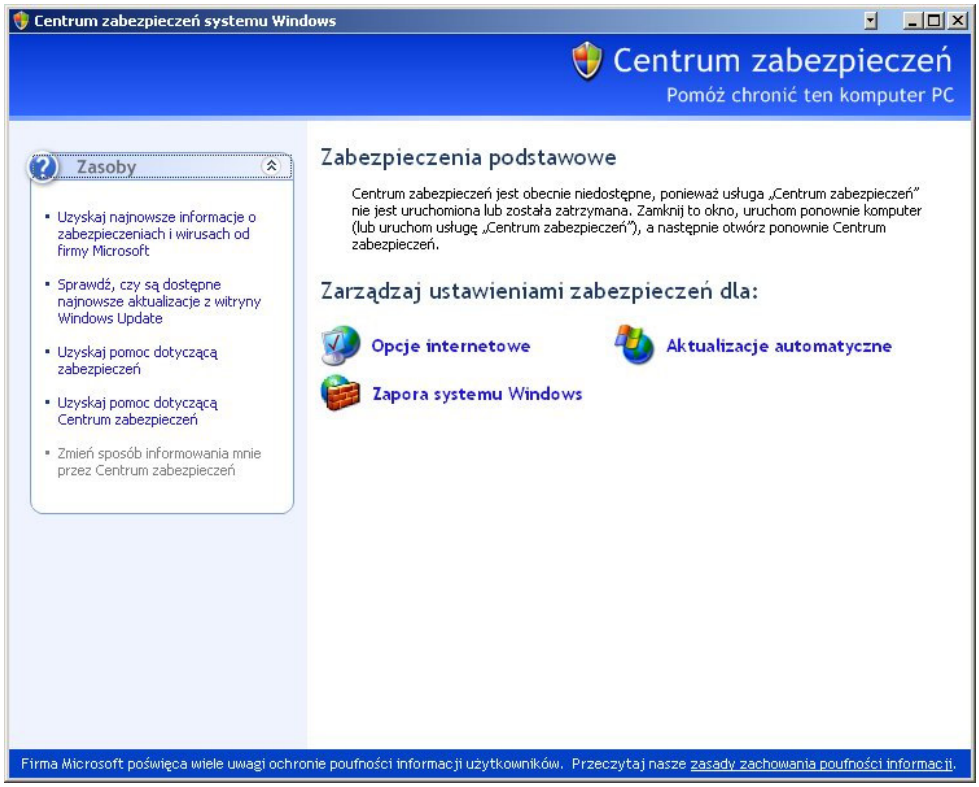
Szczegółowe informacje o stanie komunikacji sieciowej (np. informacje o aktywnych bieżąco usługach, nawiązanych połączeniach, statystyki dotyczące ruchu sieciowego) można uzyskać za pomocą polecenia `netstat`:



Rysunek 16 Wynik działania polecenie netstat.

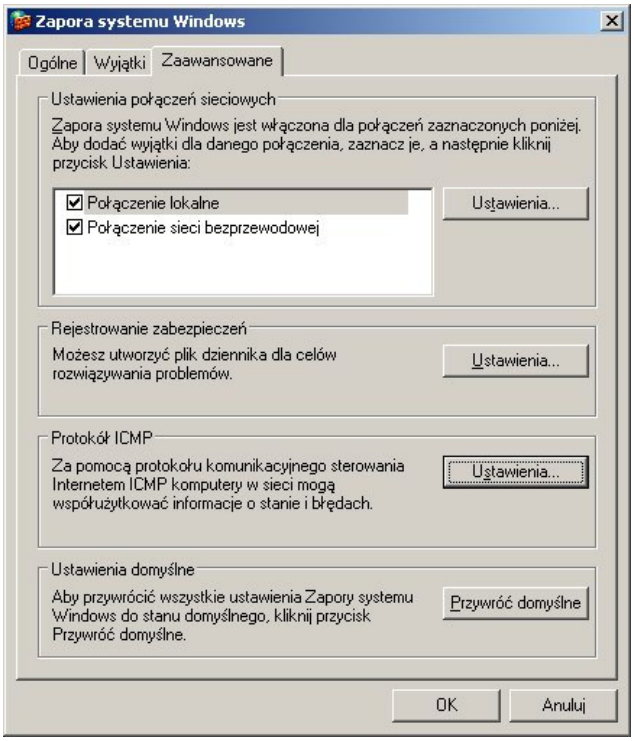
5.4 Zapory sieciowe

W systemie Windows XP SP 2 dostępne jest Centrum zabezpieczeń zawierające m.in. zaporę sieciową:



Rysunek 17 Okno Centrum zabezpieczeń systemu Windows.

Zapora wbudowana w system Windows jest bardzo prymitywna i nie daje użytkownikowi wielu możliwości:

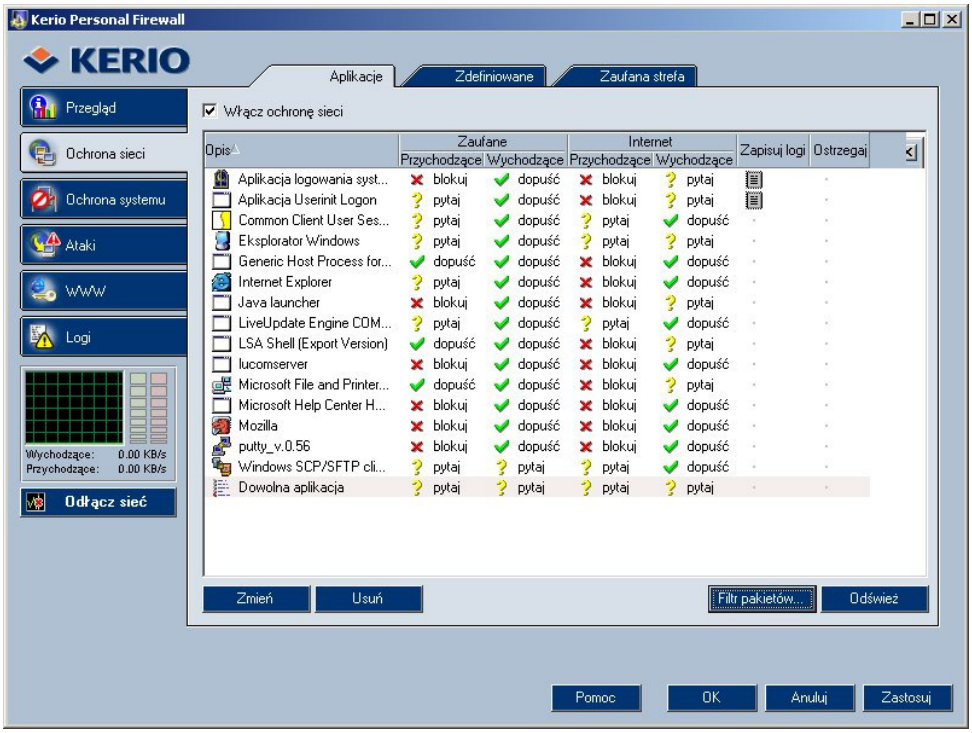


Rysunek 18 Okno konfiguracji zapory sieciowej wbudowanej w system Windows.

Zadanie:

- Zablokuj całkowicie komunikację z wykorzystaniem protokołu ICMP. Przetestuj konfigurację za pomocą polecenia `ping`.

Niestety, ta prosta zapora nie umożliwia precyzyjnej kontroli ruchu sieciowego. Z tego powodu nieodzowne stają się oddzielne produkty typu *Personal Firewall*. Dobrym przykładem może być Kerio Personal Firewall (firmy Kerio), który pozwala na wielopoziomowe filtrowanie ruchu sieciowego:



Rysunek 19 Okno programu Kerio Personal Firewall.

6 Podsumowanie

Systemy z rodziny MS Windows są bardzo popularne. Nie wszystkie elementy systemu stoją na tak wysokim poziomie jak graficzny interfejs użytkownika. W Internecie można znaleźć wiele przykładów na to iż systemy te są podatne na wiele groźnych ataków dzięki którym użytkownicy mogą być narażeni na utratę dany, szantaże i straty materialne spowodowane kradzieżą numerów kont, haseł itp. Firma Microsoft dokłada starań aby jej produkty były coraz mniej podatne na różnego typu ataki jednak nie zwalnia to użytkowników od interesowania się bezpieczeństwem systemu operacyjnego którego używają na co dzień. Dlatego też podstawowa wiedza z dziedziny szeroko rozumianego bezpieczeństwa systemów komputerowych i informacji jest konieczna do przyswojenia jeśli użytkownicy nie chcą być

biernymi obserwatorami nadużyć komputerowych popełnianych na ich systemach operacyjnych.

7 Problemy do dyskusji

- Jakie znasz ataki na które podatne są systemy z rodziny MS Windows?
- Czy wiesz jak się bronić przed najczęstszymi atakami takim jak wirusy, robaki internetowe, programy szpiegujące i spam?
- Czy znasz i używasz popularne zamienniki programów stosowanych na platformie MS Windows które są często powodem problemów z bezpieczeństwem? Czy potrafisz wymienić takie programy?

8 Bibliografia

Poniżej zostały wymienione popularne serwisy internetowe w których czytelnik znajdzie dużo informacji na temat bezpieczeństwa systemów komputerowych.

- http://hacking.pl/
- http://www.securitywortal.pl/
- http://www.bezpieczenstwoit.pl/
- http://www.jetico.com/
- http://mozillapl.org/
- http://enigmail.mozdev.org/
- http://www.thawte.com/
- http://www.kerio.com/
- http://www.cyberpatrol.com/
- http://www.insecure.org/
- http://www.nessus.org/
- http://www.eeye.com/
- http://www-arc.com/sara/
- http://www.pcflank.com/scanner1.htm
- http://scan.sygatetech.com/
- http://www.hackerwatch.org/
- http://www.testmyfirewall.com/