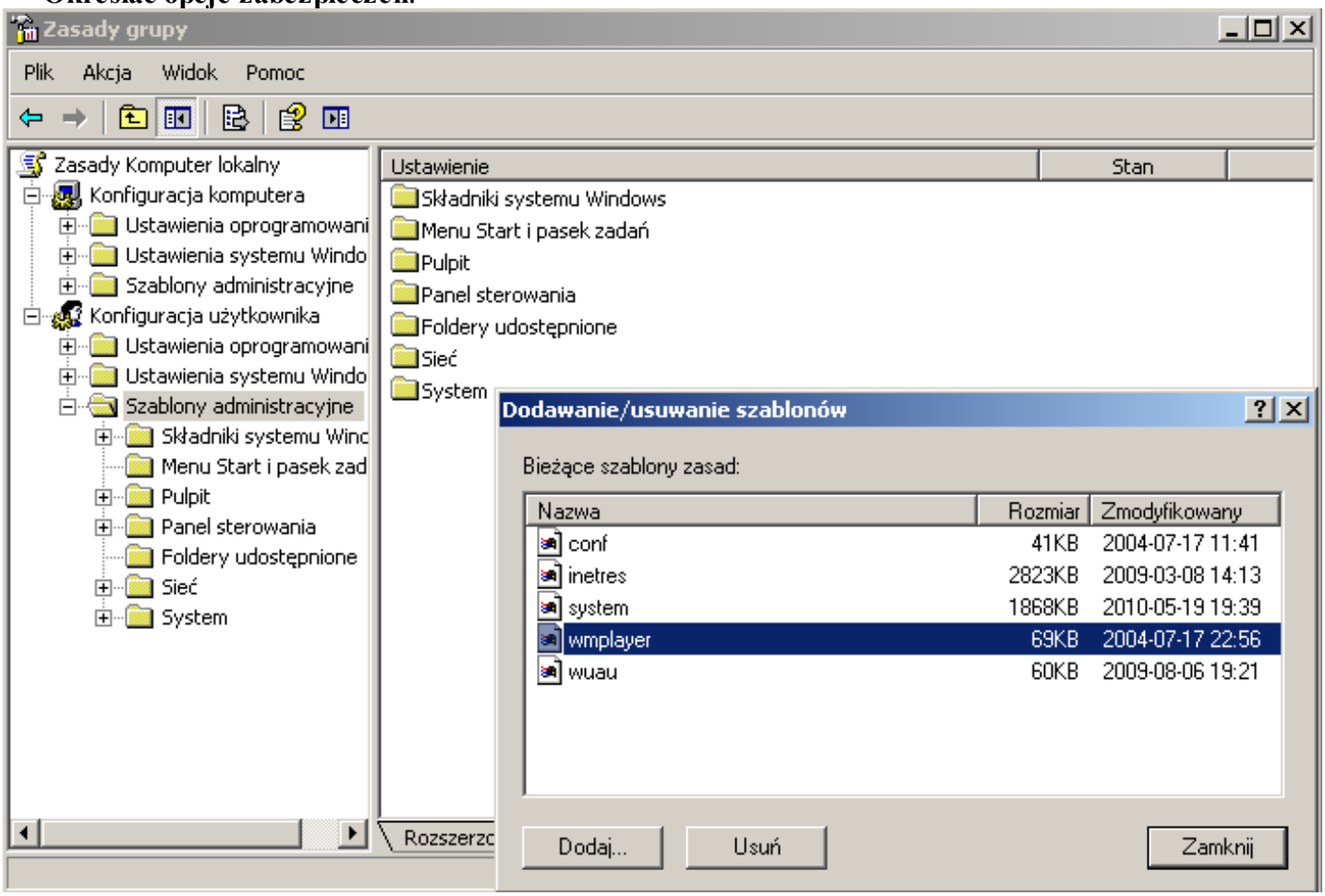
T: Zasady zabezpieczeń.

Zasady zabezpieczeń można edytować za pomocą konsoli administracyjnej **Zasady grupy** (gpedit.msc) lub otwierając pustą konsolę **mmc.exe** i dołączając do niej przystawkę **Edytor obiektów zasad grupy**. Przystawka pozwala zdefiniować ustawienia zasad, które będą stosowane do komputerów lub użytkowników. Dostępne ustawienia w konsoli Zasady grupy można dodawać bądź usuwać poprzez tzw. **Szablony administracyjne**. Aktualnie wykorzystywane w konsoli szablony administracyjne zapisane są w postaci plików z rozszerzeniem ***.adm** znajdujących się w katalogu %Systemroot%\System32\GroupPolicy\Adm. Szablony administracyjne, które możemy dodać do konsoli Zasady grupy znajdują się w systemie w katalogu %Systemroot%\inf lub możemy pobrać je bezpłatnie ze stron internetowych firmy Microsoft.

Przy użyciu przystawki Zasady grupy można wykonywać następujące czynności:

- **Zarządzać zasadami opartymi na rejestrze**, za pomocą Szablonów administracyjnych. Przystawka Zasady grupy tworzy plik zawierający ustawienia rejestru, które są zapisywane w części User lub Local Machine bazy danych rejestru. Ustawienia profilu użytkownika właściwe dla użytkownika, który loguje się na danej stacji roboczej lub serwerze, są zapisywane w rejestrze w kluczu HKEY_CURRENT_USER (HKCU), a ustawienia właściwe dla komputera są zapisywane w kluczu HKEY_LOCAL_MACHINE (HKLM).
- **Przypisywać skrypty**. Znajdują się tu takie skrypty, jak uruchamianie komputera, zamykanie komputera oraz operacje logowania i wylogowywania.
- **Przekierowywać foldery**. Można przekierować foldery, takie jak Moje dokumenty i Moje obrazy, z folderu Documents and Settings na komputerze lokalnym do lokalizacji sieciowych.
- **Zarządzać aplikacjami**. Używając rozszerzenia Instalacja oprogramowania przystawki Zasady grupy, można przypisywać, publikować, aktualizować lub naprawiać aplikacje.
- **Określać opcje zabezpieczeń**.



W celu wprowadzenia zasad dla użytkowników komputera należy zalogować się jako administrator i wprowadzić odpowiednie ustawienia zasad zabezpieczeń. Następnie każdy z użytkowników, którego mają dotyczyć wprowadzone zmiany powinien zostać zalogowany w systemie. Lokalne zasady zabezpieczeń zapisane są w pliku %Systemroot%\System32\GroupPolicy\User\Registry.pol dla użytkownika oraz w pliku

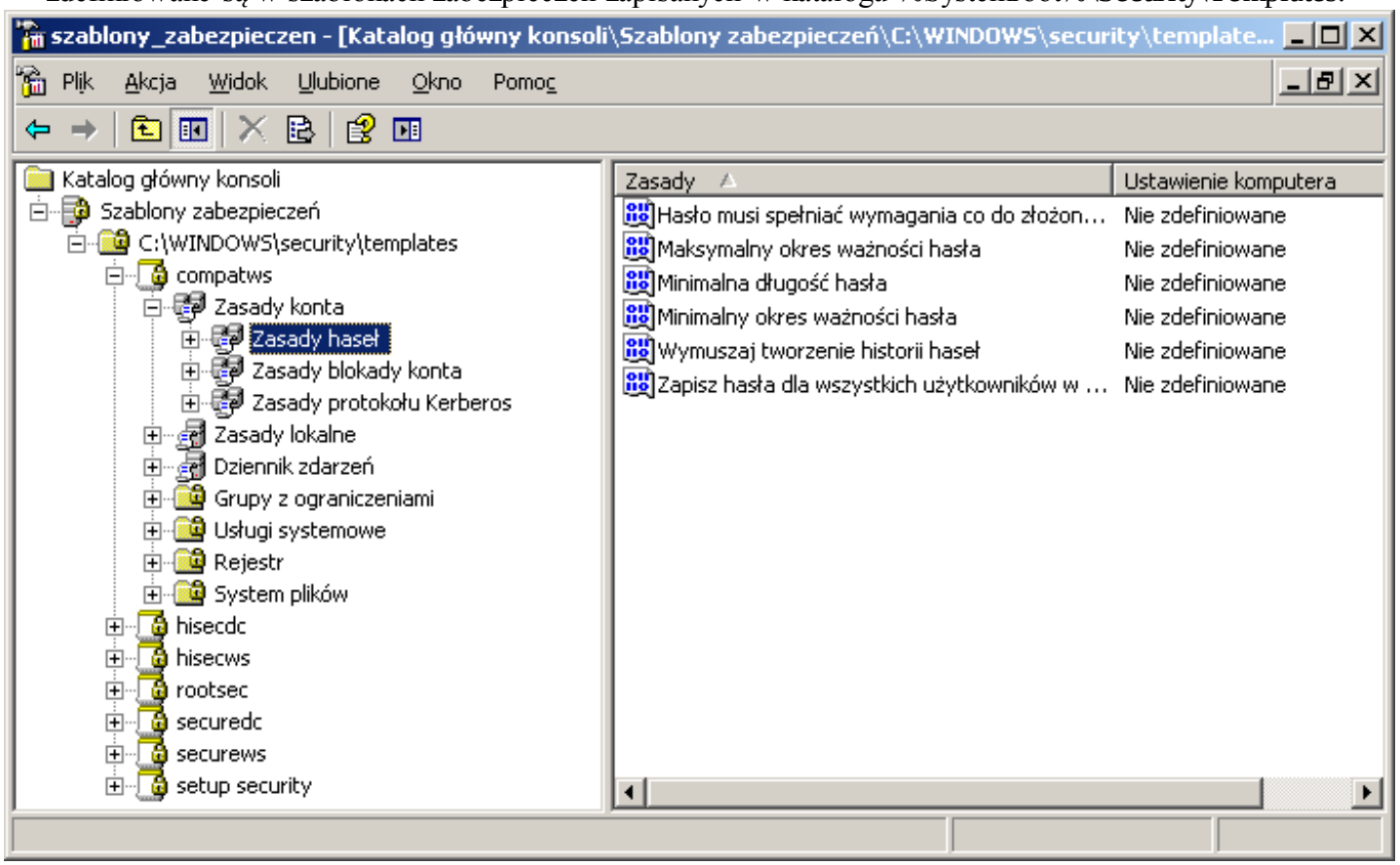
%Systemroot%\System32\GroupPolicy\Machine\Registry.pol dla komputera. Jeżeli chcemy, aby ograniczenia nie dotyczyły administratora należy po przeprowadzeniu aktualizacji zasad dla użytkowników (logowanie) zalogować się na konto administratora, skopiować plik registry.pol, powrócić do edytora zasad zabezpieczeń i cofnąć ograniczenia, zamknąć edytor zasad grup i skopiowanym wcześniej plikiem zastąpić nowy registry.pol (po zamknięciu konsoli powstał nowy plik).

W przypadku problemów z zabezpieczeniami (np. niepoprawna konfiguracja) można przywrócić ustawienia domyślne zasad grup. W tym celu należy usunąć istniejący plik registry.pol lub zmienić jego nazwę i ponownie uruchomić komputer. System ochrony plików spowoduje przywrócenie domyślnego pliku registry.pol.

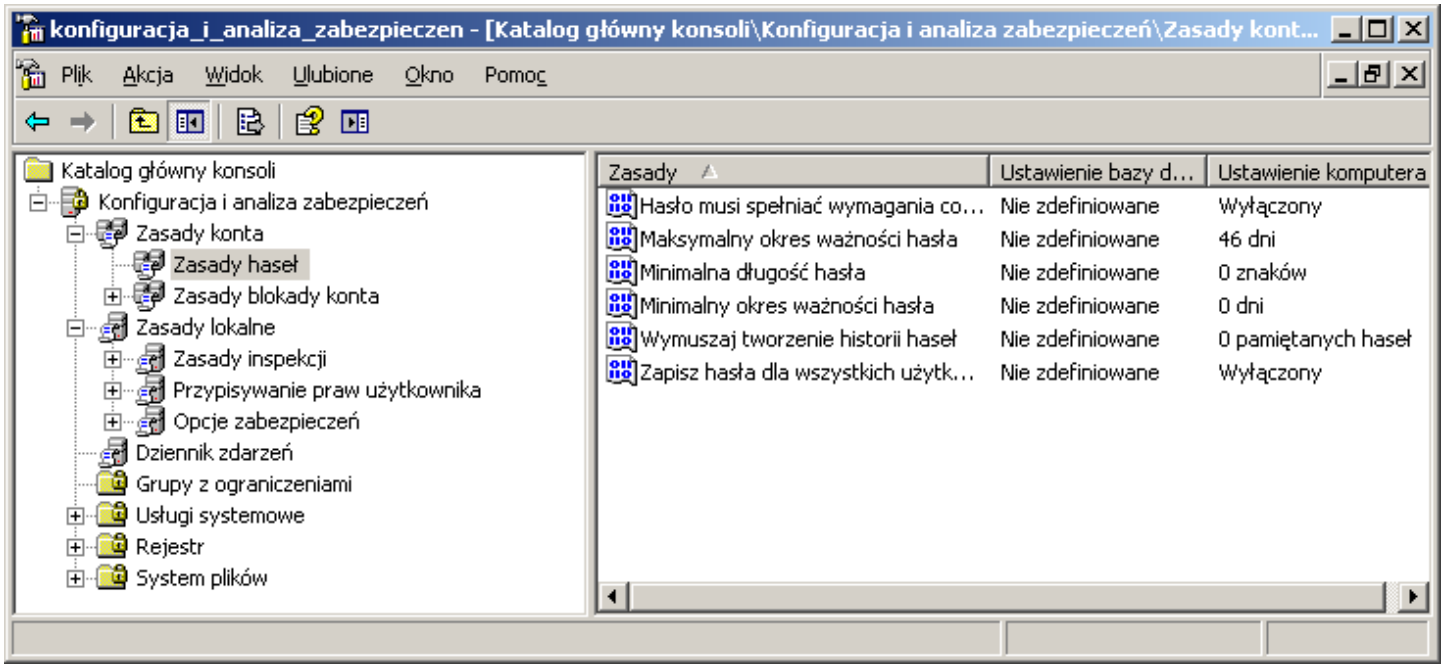
Za pomocą przystawki **Ustawienia zabezpieczeń** można modyfikować zasady zabezpieczeń jednostki organizacyjnej, domeny lub lokacji z dowolnego komputera dołączonego do domeny. Ustawienia zabezpieczeń pozwalają administratorowi zabezpieczeń modyfikować ustawienia zabezpieczeń przypisane do obiektu zasad grupy.

Wyróżniamy następujące narzędzia zasad zabezpieczeń:

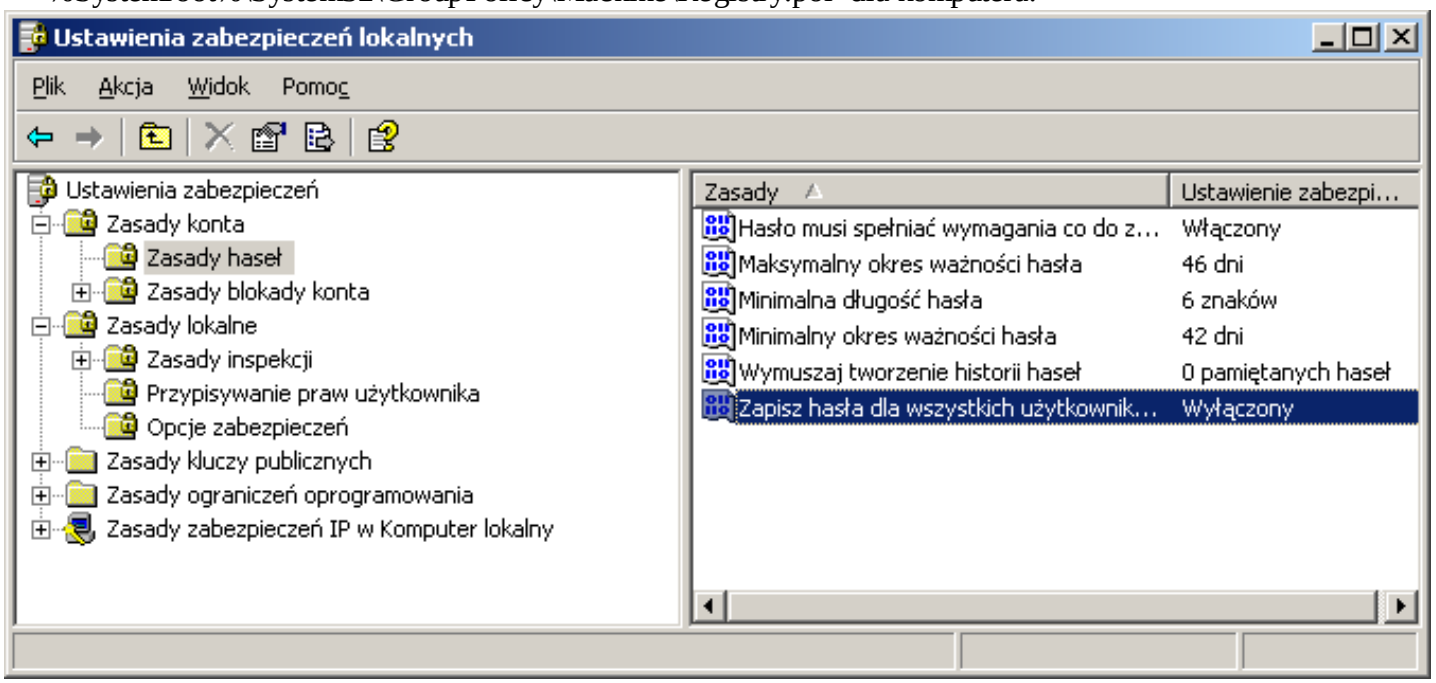
– **Szablony zabezpieczeń** - W szablonie można zdefiniować zasady zabezpieczeń. Szablony można stosować do obiektu zasad grupy lub do zabezpieczeń komputera lokalnego. Przykładowe ustawienia zabezpieczeń zdefiniowane są w szablonach zabezpieczeń zapisanych w katalogu %Systemroot%\Security\Templates.



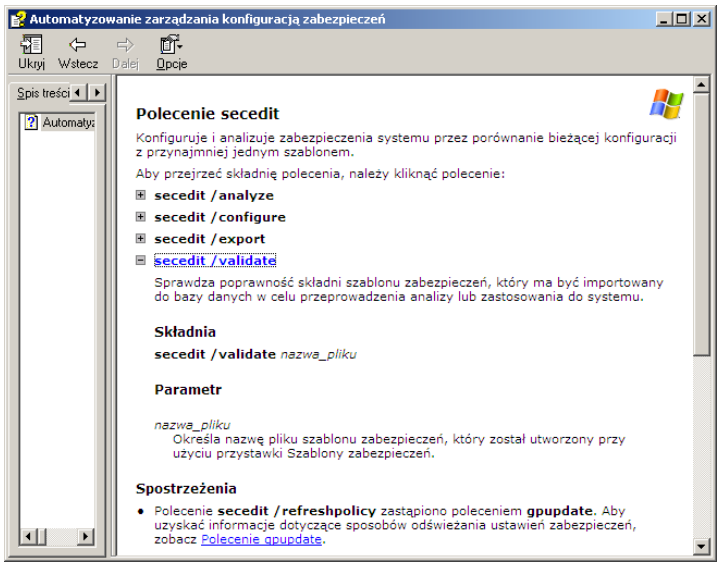
– **Konfiguracja i analiza zabezpieczeń** - Tego narzędzia można używać do konfigurowania komputera za pomocą szablonu zabezpieczeń lub do porównywania aktualnych ustawień komputera z ustawieniami zdefiniowanymi w szablonie zabezpieczeń. Niezbędne bazy danych lub szablony zabezpieczeń znajdziemy w katalogu: c:\Windows\security. Przystawka konfiguracja i analiza zabezpieczeń umożliwia przywrócenie ustawień zasad zabezpieczeń.



– **Zasady zabezpieczeń lokalnych** - Tego narzędzia można używać do edytowania poszczególnych ustawień zabezpieczeń na komputerze lokalnym. Lokalne zasady zabezpieczeń zapisane są w pliku %Systemroot%\System32\GroupPolicy\User\Registry.pol dla użytkownika oraz w pliku %Systemroot%\System32\GroupPolicy\Machine\Registry.pol dla komputera.



– **Polecenie secedit** - Tego narzędzia można używać do automatyzowania zadań związanych z konfiguracją i analizą zabezpieczeń systemu przez porównanie bieżącej konfiguracji z szablonami zabezpieczeń za pomocą wiersza poleceń.



secedit /?

secedit /configure /DB Nazwa_pliku /CFG "%windir%\Security\Templates\Setup security.inf" [/overwrite][/areasObszar1 Obszar2...] [/logŚcieżka_dziennika] [/quiet]

Porada: Do działań administracyjnych warto przygotować globalną konsolę administracyjną (za pomocą konsoli **mmc**). Taka konsola powinna zawierać następujące przystawki:
- .NET Framework Configuration,
- Dzienniki wydajności i alerty,
- Group Policy Management,
- Konfiguracja i analiza zabezpieczeń,
- Menedżer autoryzacji,
- Monitor sieci bezprzewodowej,
- Pulpity zdalne,
- Rozproszony system plików (DFS),
- Szablony zabezpieczeń,
- Przystawki do zarządzania Active Directory,
- Urząd certyfikacji,
- Usługi składowe,
- Wynikowy zestaw zasad.

W celu przygotowania konsoli należy wykonać:

```
Start => Uruchom => mmc /a %SystemRoot%\system32\compmgmt.msc
```

Spowoduje to uruchomienie konsoli Zarządzanie komputerem w trybie do edycji. Nową konsolę zapisujemy pod nową nazwą w katalogu c:\Toolkit.

Polecenia do samodzielnego przeanalizowania:
- **gpupdate /force**,
- gpresult /user login,
- konsola administracyjne gpedit.msc,
- konsola administracyjna rsop.msc.