Konfiguracja i administracja serwerem SAMBA

Wprowadzenie

Server Message Block (SMB) to protokół służący udostępnianiu zasobów komputerowych, m.in. drukarek czy plików. SMB jest protokołem typu klient-serwer, a więc opiera się na systemie zapytań generowanych przez klienta i odpowiedzi od serwera. Wyjątkiem od tej zasady jest mechanizm tzw. oplocków (opportunistic lock), w którym to serwer może wygenerować nieproszony przez klienta sygnał informujący o zerwaniu wcześniej założonej blokady. Niemniej jednak, chociaż sam protokół ma charakter klient-serwer, to z racji tego, że najczęściej maszyny klienckie dysponują także funkcjami serwerowymi (udostępnianie plików) to sieci SMB nabierają charakteru sieci peer-to-peer. Protokół SMB wykorzystuje do działania dwa protokoły niższych rzędów - protokół warstwy sesji NetBIOS (który sam wykorzystuje jako warstwę transportu TCP/IP, DECnet albo IPX/SPX) lub protokół nierutowalny NetBEUI będący protokołem warstw sieci, transportu i sesji. Systemy Microsoft Windows potrafią korzystać z SMB, a co za tym idzie NetBIOS, zarówno poprzez TCP/IP (obecnie najpopularniejsza metoda), jak i poprzez IPX/SPX, NetBEUI (stosowany tylko w małych sieciach). SaMBa instalowana na systemach Unix, korzysta tylko z SMB poprzez TCP/IP. Identyfikacja komputerów w sieciach SMB odbywa się za pomocą ich nazw NetBIOS (nazwą jest ciąg znaków, nie dłuższy niż 15 znaków) lub za pomocą mechanizmów protokołów podległych SMB, np. poprzez adres IP czy nazw DNS, gdy SMB wykorzystuje protokół TCP do transportu danych. Najczęściej z implementacją protokołu SMB spotykamy się przy okazji styczności z systemem Microsoft Windows. Każda wersja SSO Microsoft począwszy od Windows 3.11 for Workgroups zawiera implementację SMB/ Jednak nie są to jedyne implementacje. Wśród innych należy wymienić: Samba (dla systemów Unix) oraz produkty komercyjne dla systemów SCO UNIXware, SCO OpenServer, Solaris, HP-UX, OS/2 i innych.

SMB oferuje dwa modele bezpieczeństwa:

- **share level** - polegający na zabezpieczeniu zasobu i znajdujących się w nim plików hasłem. Znajomość samego hasła wystarcza do uzyskania dostępu. Jest to jedyny model np. w Windows for Workgroups, Windows 95/98/Me oraz jako jedna z możliwości w Sambie;
- **user level** - oparty na zabezpieczaniu konkretnych plików poprzez prawa dostępu przyporządkowane konkretnym użytkownikom. Znajomość użytkownika i hasła jest warunkiem do uzyskania dostępu do zasobu. Jest to jedyny model np. w Microsoft Windows z rodziny NT czyli m.in. w Windows 2000/XP/2003 oraz jako jedna z możliwości w Sambie;

Inną kwestią dotyczącą bezpieczeństwa jest podział na grupy robocze oraz poznane już na poprzednich zajęciach domeny. Dla przypomnienia zatem definicje struktur organizacyjnych reprezentowanych przez SSO.

Definicja 1

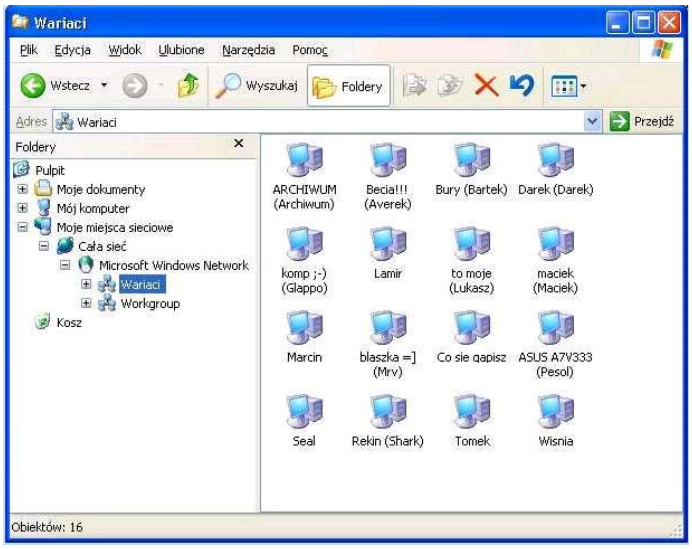
Grupa robocza to zespół komputerów, w którym na każdym z komputerów przechowywane są poufne dane oraz proces logowania, autoryzacji i uwierzytelnienia przebiega lokalnie. Rozwiązanie preferowane w sieciach domowych i w małych firmowych.

Definicja 2

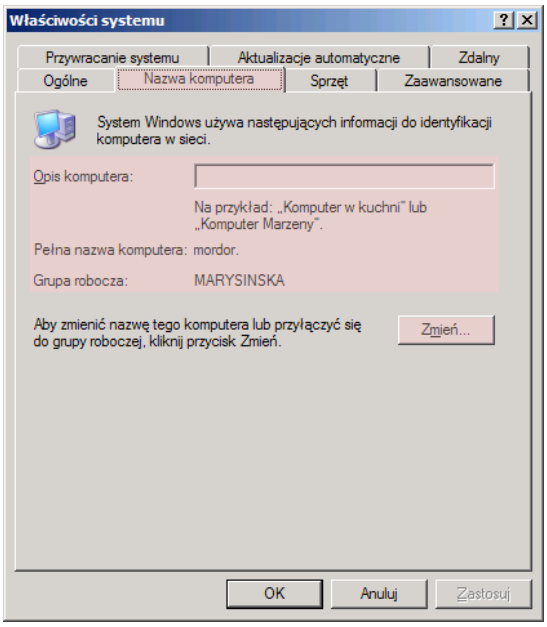
Domena prezentuje podejście scentralizowane do kwestii przechowywania poufnych danych - w każdej domenie funkcjonuje kontroler domeny (jeden główny oraz ewentualnie kilka zapasowych), przechowujący dane poufne. Procesy autoryzacji, autentykacji przeprowadzane są centralnie. Rozwiązanie preferowane w większych sieciach firmowych i korporacyjnych.

Przeglądanie otoczenia sieciowego

Systemy Windows 2000/XP/2003/2008/Vista/7 mają wbudowana obsługę przeglądania otoczenia sieciowego, umożliwiającą korzystanie z ogólnodostępnych zasobów (Rys. poniżej - przykład Windows XP). Dostęp do Otoczenia sieciowego np. w Windows XP/2003 odbywa się poprzez np. ikonę Moje miejsce sieciowe na Pulpicie. Standardowo w otoczeniu znajdują się komputery, które mają zainstalowany mechanizm Udostępnianie plików i drukarek w sieciach Microsoft Networks (systemy Windows) lub **uruchomiony demon SaMBa (systemy Linux)**.



Aby komputer zaistniał w *Otoczeniu sieciowym* musi zostać właściwie skonfigurowany. Służy do tego zakładka *Nazwa komputera*. Aby ją wywołać należy w *Panelu sterowania* kliknąć ikonę *System* i w wyświetlonym oknie wybrać zakładkę *Nazwa komputera*.



Okno konfiguracyjne umożliwia nadanie:

- **opisu komputera** - parametr opcjonalny. Tekst opisu nie powinien być dłuższy niż 48 znaków;
- **nazwy komputera** - każdemu komputerowi winna zostać nadana indywidualna nazwa. W celu zmiany parametrów należy wybrać przycisk Zmień. W polu Nazwa komputera można wykorzystać litery, cyfry i symbole @ % & * ( ) ' - . ,ale nie można zawrzeć samych kropek. Definiowana nazwa NetBIOS komputera może mieć maksymalnie długość 15 znaków. Pole Nazwa komputera pozwala na wpisanie w Windows 2000/XP/2003 aż 63 znaki,
- **członkostwa** - parametr określający grupę roboczą. Nazwa Grupy roboczej nie może mieć więcej niż 15 znaków.

W systemach Microsoft Windows 2000/XP/2003 logowanie do sieci Microsoft Networks odbywa się podczas próby korzystania z udostępnionych zasobów. Domyślnie Windows 2000/XP/2003 będzie korzystał z udostępnionych zasobów poprzez konto Gość, chyba że zdalny komputer wymusi korzystanie z konta konkretnego użytkownika zabezpieczonego hasłem. Jeśli Windows 2000/XP/2003 nie loguje się na konto Gość na zdalnej maszynie będzie próbował uwierzytelnienia przy pomocy loginu i hasła zalogowanego do systemu użytkownika. Jeśli powyższa akcja nie powiedzie się, podejmowana jest próba autoryzacja za pomocą monitu o odpowiedni login i hasło.

Połączenie z zasobami na komputerze w sieci Microsoft Network można ustanowić poprzez podanie w menu Uruchom bądź pasku adresu Explorera nazwy udziału postaci: *[Komputer]\[Zasób].*

Przykładowo: chcąc podłączyć się do zasobu Muzyka na komputerze o adresie 10.1.1.5 należy podać:

\\10.1.1.5\Muzyka

Instalacja serwisu SAMBA

administrator@ssoubuntumaster:~$ sudo apt-get install samba

Konfiguracja serwisu SAMBA

Pierwszą czynnością jaka należy zrobić jest sprawdzenie czy w pliku */etc/services* znajdują się następujące linie:

```
netbios-ns      137/tcp                 # NETBIOS Name Service
netbios-ns      137/udp
netbios-dgm     138/tcp                   # NETBIOS Datagram Service
netbios-dgm     138/udp
netbios-ssn     139/tcp                 # NETBIOS Session service
netbios-ssn     139/udp
```

Upewnijmy się, że wszystkie są odkomentowane. W zależności od dystrybucji, możliwe, że będziemy musieli je dodać. Samba nie będzie w stanie dowiązać się do odpowiednich portów, jeśli tych linii nie będzie w powyższym pliku.

Ręcznie demony można uruchomić komendami:

/usr/sbin/smbd -D
/usr/sbin/nmbd -D

Jednakże bezpieczniejszym rozwiązaniem jest użycie skryptu startowego. W Ubuntu Linux uruchomić serwer można poleceniem:

/etc/init.d/samba start | restart

Natomiast zatrzymać można poleceniem:

/etc/init.d/samba stop

Plik konfiguracyjny

Konfiguracja Samby jest kontrolowana jednym plikiem: /etc/samba/smb.conf. W pliku tym umieszczamy zasoby jakie chcemy udostępnić dla świata (lub naszej sieci lokalnej) i jakie restrykcje chcesz wprowadzić. Po zainstalowaniu Samby plik /etc/samba/smb.conf nie istnieje lub jest pusty. Przykładowa konfiguracja znajduje się w pliku /etc/samba/smb.conf.example.

Dobrym pomysłem jest rozpoczęcie pracy od skopiowania pliku przykładowego pod nazwa smb.conf.

Każda sekcja pliku zaczyna się od nazwy jak np.: *[global]*, *[homes]*, *[printers]* itp.

Sekcja [global] - parametry ogólne

Sekcja *[global]* definiuje kilka ogólnych zmiennych, które będą się odnosić do wszystkich udostępnianych zasobów. Przykładowy wpis dla tej sekcji może mieć postać:

```
[global]
 workgroup = moja_grupa_robocza
 netbios name = moj_komputer
 server string = Mój serwer linuksowy
 guest account = nobody
 log file = /var/log/samba-log.%m
```

workgroup
: określa grupę roboczą w otoczeniu sieciowym

netbios name
: określa nazwę NetBIOS

server string
: określa opis komputera w otoczeniu sieciowym

guest account
: określa użytkownika, który będzie używany podczas logowań anonimowych

log file
: określa plik do którego zostaną zapisane informacje o zarażeniach

Sekcja [udział] - konfiguracja dowolnego udziału

Aby dodać nowy udział należy utworzyć sekcję o nazwie identycznej z zasobem, który będziemy wykorzystywali. Na przykład:

```
[testowy]
 comment = Udział testowy
 path = /mnt/testowy
 create mask = 0777
 directory mask = 0777
 browsable = yes
 writeable = yes
 guest ok = yes
```

testowy
: określa nazwę udziału

comment
: określa opis wyświetlający się w otoczeniu sieciowym

path
: określa ścieżkę dostępu do danych

create mask
definiuje z jakimi prawami pojawią pliki utworzone przez sieć (=create mode)
directory mask
definiuje z jakimi prawami pojawią katalogi utworzone przez sieć (=directory mode)
browsable
określa czy udział ma byś widoczny dla klientów (=browsable)
writeable
określa czy istnieje możliwość zapisu (=writeable, !=read only)
guest ok
określa, iż zasób może być używany przez gościa (=public)

Sekcja [homes]
Sekcja *[homes]* pozwala użytkownikom na dostęp do ich (i tylko ich) katalogów domowych na lokalnej maszynie Linuksowej. Jeśli jakiś użytkownik Windows będzie chciał skorzystać z udostępnianych zasobów, to zostanie podłączony do swojego katalogu domowego. Zauważmy, że aby to zrobić użytkownik musi mieć swoje konto na maszynie Linuksowej. Przykład konfiguracji katalogów domowych:

```
[homes]
 comment = Katalogi Domowe
 browseable = no
 read only = no
 create mode = 0750
```

Po stworzeniu nowego pliku smb.conf dobrze jest zweryfikować czy jest poprawny. Można to zrobić przy pomocy programu ***testparm***. Jeśli program ten nie zgłosi żadnych błędów, to smbd poprawnie załaduje ten plik.

Jeśli Wasz serwer Samba ma więcej niż jeden interfejs ethernet, demon smbd może dołączyć się do złego. Jeśli tak się stanie, to możemy zmusić smbd do dowiązania się do dobrego przez dodanie do sekcji [global] poniższej linii:

interfaces = 192.168.1.1/24

Tworzenie użytkowników

Użytkownik serwera SMB powinien najpierw zostać utworzony w systemie Linux. np.:

adduser nowy_uzytkownik

Starsze wersje Samby domyślnie obsługiwały użytkowników systemu zdefiniowanych w /etc/passwd. Niestety w ramach zwiększania poziomu bezpieczeństwa Microsoft zmienił w nowych wersjach Windows sposób kodowania haseł. Aby zachować kompatybilność z nowymi wersjami systemów MS, Samba przechowuje hasła w dodatkowym pliku smbpasswd. Samba od wersji 3.x korzysta z tego pliku oraz kodowanych haseł domyślnie. Z tego powodu, aby użytkownik mógł korzystać z serwera w celu ustawienia hasła dla protokołu SMB należy wydać komendę:

smbpasswd -a nazwa_uzytkownika

Zadania

1. Zainstalujcie, skonfigurujcie i uruchomie serwer SMB w SSO Ubuntu Linux;
2. Utwórzcie udziały udzial1 i udzial2;
3. Utwórzcie użytkowników smb1 i smb2;
4. Utwórzcie udział homes, który przyłączy katalog domowy zalogowanego użytkownika;
5. Użyjcie udziałów udostępnionych przez Sambę w systemie Windows XP np. utwórzcie pliki tekstowe w katalogu testowy (lub innym) i spróbujcie je odczytać oraz coś do nich zapisać;

Oczywiście tworząc pliki pamiętamy o nadaniu w Linuxie niezbędnych praw do plików i katalogów udostępnianych przez Sambę.

Programy narzędziowe SMB

smbclient

Programem służącym do przeglądania zasobów SMB na innych komputerach jest *smbclient*. Narzędzie działa analogicznie do standardowych klientów protokołu FTP. Aby połączyć się z serwerem plików należy wydać komendę:

smbclient *adres**udział -Uuzytkownik*

lub

*smbclient '**adres**udział' -Uuzytkownik*

lub

smbclient //adres/udział -Uuzytkownik

Niemożność zastosowania typowej notacji Windows (adres/udział) wynika z tego, iż znak \ interpretowany jest przez większość powłok Unix. Aby powłoka przekazała do programu znak \ należy wpisać \\ lub ująć tekst w apostrof.

Komendy programu są identyczna jak w typowych klientach FTP. Spis poleceń można uzyskać wpisując polecenie h.

Listę zasobów danego serwera możemy uzyskać wydając polecenie:

smbclient -L nazwa_serwera

findsmb

Wyszukuje dostępne serwery SMB

smbstatus

Polecenie pozwala na wyświetlenie informacji o stanie serwera plików.

smbcontrol

Polecenie pozwala na zarządzanie zasobami SMB. Jest ono odpowiednikiem Windowsowego polecenia NET. Uwaga: najnowsze wersje Samby oferują także polecenie NET.

smbmount

System Linux potrafi zamontować (przyłączyć do drzewa katalogów) dysk sieciowy cifs w sieci SMB (Microsoft Networks) pod warunkiem że jest zainstalowany pakiet samba oraz że w używany kernel (jądro systemu) obsługuje cifs, czyli albo ma wkompilowane na stałe lub jako moduł (wtedy trzeba go załadować). Oczywiście w większości popularnych dystrybucji nie powinieneś na standardowym kernelu otrzymać komunikatu w stylu "cifs filesystem not supported by the kernel", gdyż taka obsługa zazwyczaj już jest.

Montowanie zasoby cifs wykonujemy np. taką komendą:

mount -t cifs -o guest //komp/udzial /mnt/mountpoint

montujemy tutaj jako gość katalog *udział* znajdujący się na *komp* umieszczając go w naszej strukturze katalogów w miejscu */mnt/mountpoint*

mount -t cifs -o username="user",password="hasło" //komp/udział /mnt/mountpoint

montujemy tutaj jako użytkownik *user* z hasłem *hasło* katalog *udział* znajdujący się na *komp* umieszczając go w naszej strukturze katalogów w miejscu */mnt/mountpoint*

Do automatycznego montowania udziałów możemy użyć wpisu w pliku */etc/fstab*. Na przykład aby zamontować zasób na konto Gość z możliwością zapisu należy w */etc/fstab* wpisać:

//komp/udzial /mnt/mountpoint cifs guest,fmask=777,dmask=777 0 0

Aby określić hasło z jakim udział zostaje zamontowany w */etc/fstab* należy wpisać:

//komp/udzial /mnt/mountpoint cifs username="user",password="mojehasło" 0 0

Zadania

1. Utwórz udział w systemie Windows XP i przy pomocy smbclient pobierz z niego plik.
2. Zamontuj udział w drzewie katalogów w */mnt/windowsxp*