Konfiguracja serwera pocztowego

Autorzy: Barbara Słonina, Piotr Sudia, Piotr Szczypek IVFDS

STRESZCZENIE

Celem naszej pracy jest zainstalowanie systemu operacyjnego Linux Debian 3.0 a następnie zaimplementowanie usługi poczty elektronicznej. Źródłem pakietów instalacyjnych były płyty z dystrybucją. Po określeniu konfiguracji sieci zajęliśmy się instalacją oraz edycją plików konfiguracyjnych, przy wykorzystaniu wbudowanego edytora Midnight Commander'a. Skonfigurowaliśmy lokalne oraz zewnętrzne dostarczanie poczty. Programem, który wybraliśmy na serwer pocztowy był postfix. Aby go skonfigurować stworzyliśmy alias pocztowy dla konta administratora serwera root oraz określiliśmy domenę, dla której demon ma odbierać pocztę. Aby zapewnić odbiór poczty z sieci lokalnej doinstalowaliśmy usługę pobierania poczty pop3 instalując pakiet ipop3 – serwis ten działa pod kontrolą demona xinetd.

SPIS TREŚCI

Streszczenie 1
Wstęp 3
1.1. Poczta elektroniczna 3
1.2. Potrzebne programy 4
1.3. Adres e-mail 4
2. Konfiguracja serwera pocztowego 5
2.1. Pod kontrolą systemu operacyjnego Linux 5
2.2. Pod kontrolą systemu Windows 2000 7
3. Protokoły poczty 9
3.1. Protokół POP 10
3.2. Protokół IMAP 10
3.3. Protokół SMTP 11
4. Ochrona antyspamowa 12
5. Ochrona antywirusowa 13
Literatura 15

WSTĘP

Debian GNU/Linux 2.2 (Potatoe) był dystrybucją systemu Linux, na której konfigurowaliśmy usługę sieciową (daemon). Źródłem pakietów instalacyjnych były płyty z dystrybucją.

Dystrybucja Debian GNU/Linux należy do jednych z trudniejszych w konfiguracji spośród licznych dystrybucji systemu operacyjnego Linux.

Systemy Debian używają obecnie jądra Linux. Jest to wolne (w sensie braku ograniczeń, a nie szybkości) oprogramowanie, które zaczął tworzyć Linus Toryalds, a którym obecnie zajmują się tysiące programistów z całego świata.

1.1. Poczta elektroniczna

Pierwszy program do przesyłania wiadomości stworzył już w 1972 roku Ray Tomilson. Jego nazwa to SNDMSG, co jest skrótem od send message, czyli wyślij wiadomość. Aplikacja ta dała początek wielu kolejnym programom, co spowodowało konieczność standaryzowania procesu wysyłania informacji w sieci.

Pierwszym dokumentem który tego dokonał był, wydany pod koniec lat siedemdziesiątych "Mail Transfer Protocol" (protokół przekazywania poczty). Kolejnym krokiem w etapie udoskonalania protokołu poczty elektronicznej był, powstały w 1981 roku "Simple Mail Transfer Protocol" .

Kolejnym godnym odnotowania dokumentem był wydany w roku 1993 protokół "SMTP Service Extensions", który jednak niczego nie zmieniał w specyfikacji samego standardu a tylko wprowadzał pewne poprawki i dodatkowe możliwości.

Poczta elektroniczna (z języka angielskiego: e-mail" lub "electronic mail") jest osobistym połączeniem z siecią. Jest jedną z najwcześniejszych usług sieci Internet. Wiele milionów osób korzystających z Sieci posiada swoje własne adresy pocztowe. Rosnąca ilość bramek pocztowych powoduje, iż każdego dnia wzrasta liczba osób mogących korzystać z pocztę elektronicznej w Internecie.

Usługa przeznaczona początkowo wyłącznie do przesyłania krótkich informacji tekstowych w kodzie ASCII (alfabet łaciński, cyfry i kilkanaście znaków interpunkcyjnych), aktualnie umożliwia przesyłanie tekstów napisanych w alfabetach narodowych oraz dołączanie do nich tzw. załączników - plików binarnych zawierających programy komputerowe, dźwięk, obrazy, animacje, dane w różnych formatach i wiele innych. Należy jednak zdawać sobie sprawę, że ze względu na historyczne wymogi protokołu służącego do przesyłania poczty elektronicznej, dane binarne dołączane do przesyłek są przez programy pocztowe automatycznie kodowane do postaci tekstowej, tak by informacja przesyłana siecią składała się wyłącznie z liter cyfr i znaków interpunkcyjnych. W większości przypadków zakodowany w ten sposób plik binarny zwiększa swoją długość, co wiąże się ze zwiększeniem długości całej przesyłki. Z drugiej strony, większość komputerów uczestniczących w przesyłaniu poczty elektronicznej, nakłada limity na maksymalną długość przesyłki.

Z założenia poczta elektroniczna jest bardzo podobna do zwykłej poczty (listy, widokówki), którą wysyła się do znajomych czy przyjaciół. Poczta elektroniczna, którą wysyłasz do znajomych, przesyłana jest na ich prywatny (unikalny) adres. Podobnie, gdy oni odpisują do Ciebie, poczta kierowana jest na Twój prywatny adres.

Poczta elektroniczna ma dwie zasadnicze przewagi nad zwykłą pocztą. Najważniejszą z nich jest prędkość. W przeciwieństwie do zwykłej poczty, gdzie listy "idą" kilka dni bądź tygodni, twoje przesyłki dostarczane są do adresata w ciągu kilku, kilkunastu minut (w zależności od stanu technicznego sieci).

Drugą cechą wyróżniającą pocztę elektroniczną jest możliwość wykorzystywania tejże poczty do przeglądania baz danych, katalogów, przesyłania plików.

1.2. Potrzebne programy

MUA (Mail User Agent), MTA (Mail Transfer Agent) oraz MDA (Mail Delivery Agent) – te trzy rodzaje oprogramowania są niezbędne do poprawnego działania poczty elektronicznej, ponieważ właśnie w podanej wyżej kolejności wiadomość email wędruje pomiędzy tymi trzema agentami.

Pierwszy z nich to nic innego jak klient poczty elektronicznej, najbardziej znany dla przeciętnego użytkownika. Jego funkcje to przede wszystkim tworzenie, wysyłanie oraz czytanie wiadomości. Pozostałe czynności wykonywane często przez programy MUA to np. pobieranie wiadomości, tworzenie i zarządzanie skrzynkami pocztowymi umieszczonymi na dysku twardym, przekazywanie gotowych do wysłania e-maili do odpowiedniego programu MTA, sortowanie i filtrowanie poczty. Najpopularniejszym chyba programem tego typu w środowisku windowsowym jest Outlook Express.

Gdy już nastąpi utworzenie wiadomości, gotowej do przesłania, trafia ona do kolejnego ogniwa w łańcuchu czyli programu MTA, który z reguły znajduje się na serwerze, udostępniającym skrzynki internetowe. Zadaniem tego programu jest przesłanie, za pomocą protokołu SMTP , wiadomości do kolejnych serwerów. Ostatnim etapem jest dotarcie emaila do serwera odbiorcy. Najczęściej spotykanym tego typu programem jest UNIX-owy serwer Sendmail.

Ostatni etap to dostarczenie wiadomości do odpowiedniej skrzynki odbiorczej adresata, czyli konkretnie mówiąc jest to nic innego jak miejsce na dysku twardym, skąd , za pomocą programu MUA można daną wiadomość można odczytać czy też pobrać. Za dostarczanie listów odpowiedzialny jest program z grupy MDA, którego przykładem jest UNIX-owy program Procmail, a podobne zadanie może również pełnić sendmail. Ważną cechą jest jednak, że do odbierania początkach wysyłania poczty wystarczą same programy MUA oraz MTA.

Na początku istnienia poczty charakterystyczne było, że oprogramowanie MUA znajdowało się na komputerach, które były też maszynami odbierającymi wiadomości. Ponieważ początkach biegiem czasu sytuacja zmieniła się na rzecz komputerów „domowych", co wymusiło powstanie protokołu dostępu do poczty znajdujących się na odległych komputerów. początkach ten właśnie sposób powstały protokoły POP (Post Office Protocol) i IMAP (Internet Message Access Protocol)

1.3. Adres e-mail

Każdy adres pocztowy np. piotr@prz.rzeszow.pl składa się z następujących elementów:
- część lokalna (czyli nazwa skrzynki pocztowej), tutaj: piotr;
-"małpa" ("@");
- domena, tutaj: prz.rzeszow.pl;

Ważną cechą adresu jest to, że duże i małe litery nie są tu rozróżniane, ale nie można stosować polskich znaków. Przed samym adresem można również dodać pewne dodatkowe informacje, np. Piotr Studia <piotr@prz.rzeszow.pl>.

Istnienie również możliwość wysyłania wiadomości do grupy użytkowników, czego przykładem jest adres postaci: Studenci: piotr@prz.rzeszow.pl, baska@prz.rzeszow.pl. Z drugiej strony możliwość ta jest niejednokrotnie wykorzystywana przez rozsyłaczy spamu, ponieważ część po dwukropku jest opcjonalna.

Jak naprawdę wygląda wiadomość email

Składa się ona z kilku, dokładnie określonych przez dokumenty, części:
- nagłówek, który składa się z informacji na temat nadawcy, odbiorcy, daty nadania wiadomości oraz temat. Jest to podstawowa część całego listu, ponieważ zawiera dane bez których wiadomość nigdzie nie dotarłaby;

- treść wiadomości, ciekawą rzeczą jest jego opcjonalność, podczas gdy nagłówek jest częścią wymaganą.

Taka wiadomość jest już gotowa do przekazania programowi MTA, który zajmie się jej dostarczeniem do adresata. Każdy program MTA dodaje do wiadomości pole Received. Jest ono ważne podczas diagnozowania problemów z dostarczaniem poczty. Pozycje te to informacje o tym, kiedy list został wysłany, jaką trasę przebył i w jaki sposób można go odesłać do nadawcy. Do tej kategorii należą więc pola Date, Received oraz Return-Path. Wiadomość może spotkać na swojej drodze więcej niż dwa MTA, przykładowo dotarła ona do adresata z dużym opóźnieniem. Aby określić gdzie tkwił problem należy sprawdzić pola Received, które zawierają datę oraz czas pojawienia się wiadomości na każdym komputerze.

Cały przedstawiony proces analizy został przeprowadzony przy założeniu, że zegary wszystkich komputerów uczestniczących w przesyłaniu listu były poprawnie ustawione. W przeciwnym przypadku nie bylibyśmy w stanie wyciągnąć jakichkolwiek wniosków z nagłówka e-maila.

2. KONFIGURACJA SERWERA POCZTOWEGO

2.1. Pod kontrolą systemu operacyjnego Linux

Poczta elektroniczna jest w dalszym ciągu najważniejszą usługą dla użytkowników sieci. WWW tworzy większy ruch, ale poczta elektroniczna jest usługą używaną do większości komunikacji osobistej. Komunikacja osobista jest prawdziwą podstawą biznesu. Żadna sieć nie będzie kompletna bez poczty elektronicznej i żaden system operacyjny dla serwera sieciowego nie jest wart swojej nazwy, jeżeli nie zawiera pełnej obsługi poczty TCP/IP.

Programem, który wybraliśmy na serwer pocztowy był postfix. Jest on pakietem nastawionym na bezpieczeństwo, szybkość i łatwość konfiguracji. Ciekawą formą zabezpieczenia jest to, że serwer pracuje w wydzielonym systemie katalogów. Aby poprawić szybkość można wprowadzić algorytm wysyłania na raz tylko określonej ilości poczty oraz ograniczenie liczby procesów przesyłowych i ich wielokrotne wykorzystywanie. Cechą Postfixa jest również jego kompatybilność z pakietem Sendmaila. Posiada on ponad sto parametrów konfiguracji, które są kontrolowane przez plik main.cf. Na szczęście mają one rozsądne wartości domyślne.

Na początku usuwamy domyślny serwer pocztowy jakim jest exim. Robimy to za pomocą narzędzia apt:

```
# apt-get –purge remove exim
```

Następnie przechodzimy do instalacji serwera pocztowego:

```
# apt-get install postfix
```

Należy sprawdzić czy mamy plik /etc/postfix/main.cf. Jeżeli go nie ma należy go utworzyć.

Ustawiamy w nim m.in. dopuszczalne adresy odbierania poczty oraz domyślny adres poczty wychodzącej.

```
#odbieraj (akceptuj) pocztę dla nazwy tego hosta, lokalnie oraz
dla całej domeny
```

```
mydestination = #myhostname, localhost.$mydomain,$mydomain
```

Parametr ten wskazuje posfixowi jakie nazwy ma uważać jako domeny pocztowej. Oznacza to, że jeśli oprócz standardowej nazwy hosta jest jeszcze inna, to należy ją tu wpisać, jeśli chcemy otrzymać pocztę wysłaną na adres z tej nazwy.

```
#adres poczty wychodzącej to
uzytkownik_poczty@nazwa_domeny_serwera
myorigin = $mydomain
```

Opcja ta definiuje nazwę, która pojawia się w mail'u wysyłanym przez użytkownika. Zaleca się pozostawienie wartości $myhostname.

Inne parametry to:

```
myhostname = nazwa_hosta
```

Parametr ten opisuje nazwę naszego komputera. Może być taka sama jak nazwa domeny. Możemy ją znaleźć w /etc/host. W naszym przypadku jest to: debian5.

```
mydomain = nazwa_domeny
```

Podaje nazwę domeny, u nas jest to: debian5.prz.rzeszow.pl. Też można ją znaleźć w /etc/host

```
relay_domains = $mydestination
```

Określa z jakich komputerów możemy przekazywać pocztę.

```
mynetworks = 127.0.0.0/8  212.182.41.0/26
```

Wskazuje adresy sieci, z których możemy przesyłać pocztę.

```
queue_directory = /var/spool/posfix
```

Tu znajdują się wszystkie maile.

```
command_directory = /usr/sbin
```

Miejsce na binaria.

```
daemon_directory = /usr/lib/postfix
```

Miejsce na demony.

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
setgid_group = postdrop
biff = no

append_dot_mydomain = no
```

Powyższe ustawienia powodowały, że poczta wychodząca posiadał adresata użytkownik@prz.rzeszow.pl.
Po takim skonfigurowaniu postfixa zrestartowaliśmy go za pomocą polecenia *postfix reload*.

Następnie w celu odbierania poczty przez zdalne hosty zainstalowaliśmy pakiet pop3d:

```
apt-get install solid-pop3d
```

Serwis ten działa pod kontrolą demona xinetd. Wymaga on odblokowania dostępu dla zaufanych maszyn w plikach/etc/hoss.deny oraz /etc/hoss.allow. W naszym przypadku udostępniliśmy wszystkie usługi dowolnej maszynie z sieci wewnętrznej jak i zewnętrznej

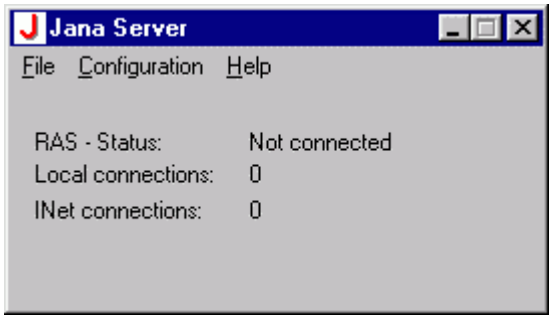
przez dodanie komentarza: ALL:ALL EXCEPT 127.0.0.1:DENY w pliku /etc/hoss.deny pozostawiając plik /etc/hoss.allow bez zmian. Pakiet pop3d jest włączany domyślnie, więc nie wymaga dodatkowej konfiguracji.

2.2. Pod kontrolą systemu Windows 2000

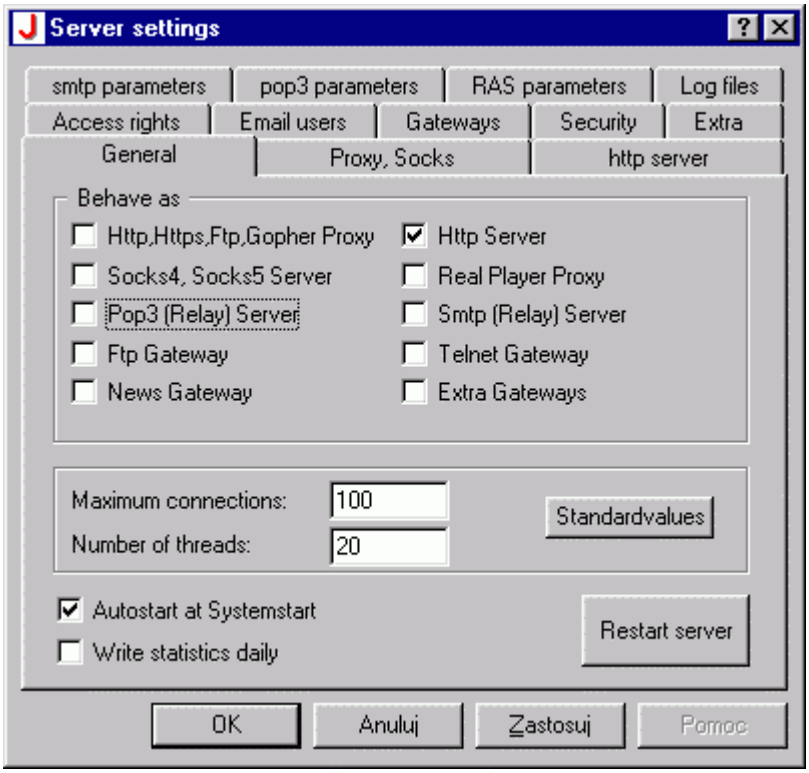
Ponieważ windows 2000 nie udostępnia standardowo serwera POP3, odpowiedzialnego za odbieranie poczty, a tylko serwer SMTP do wysyłania poczty, dlatego najlepszym rozwiązaniem jest zainstalowanie specjalnego programu np. Jana serwer, który tę opcję posiada.

Konfiguracja przebiega następująco:

- po zainstalowaniu programu konieczny jest restart systemu;
- gdy system załaduje się nasz serwer jest już uruchomiony: ikona w pasku zadań;
- przy pierwszym uruchomieniu konieczne jest wprowadzenie hasła administratora, który zarządza serwerem;
- program wygląda następująco:

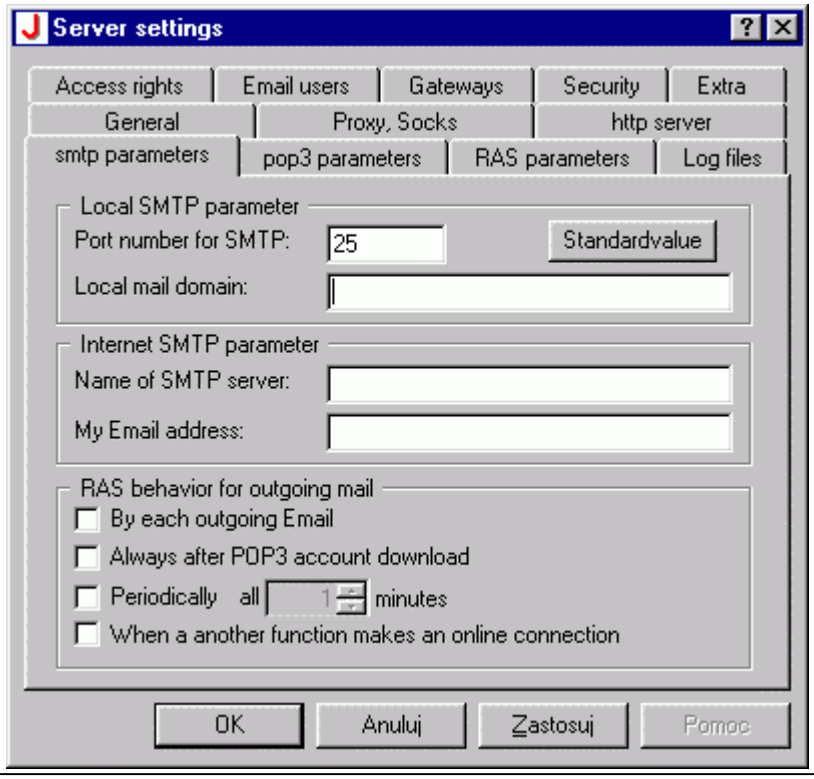


- wybieramy zakładkę: Configuration/Configuration i otrzymujemy całą paletę możliwości:

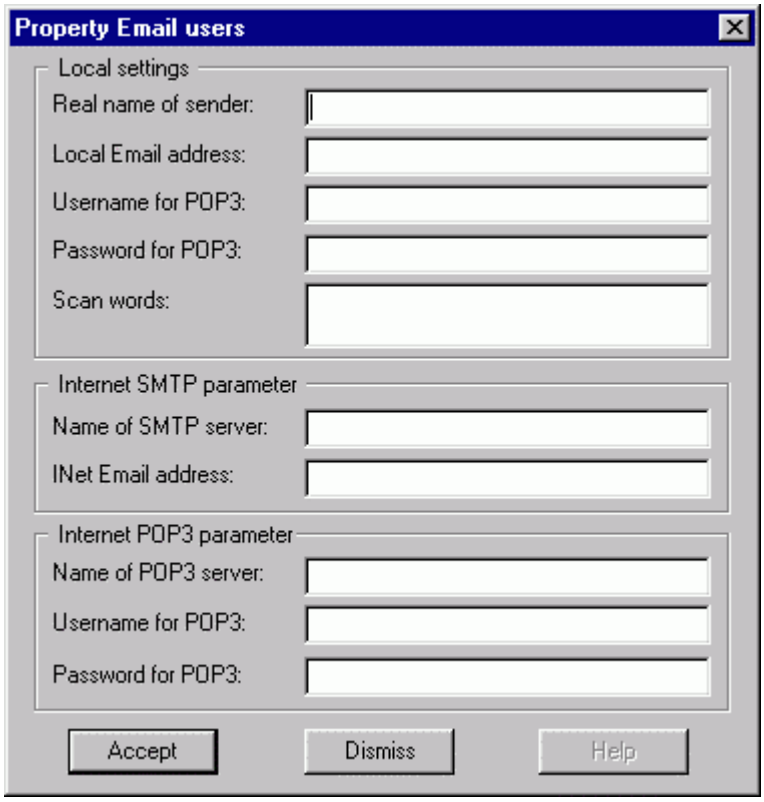


- w grupie General określamy jakie usługi będziemy wykorzystywać, jak widać jest ich sporo, należy wybrać dwie z nich: Pop3 oraz Smtp;

- teraz należy wybrać kartę Smtp parameters i określamy domenę w polu local main domain, np. prz.rzeszow.pl;



- serwer jest już prawie gotowy, należy jeszcze określić skrzynki dla użytkowników;
- należy wybrać zakładkę email users a w niej pole add:



- teraz trzeba tylko uzupełnić pola odpowiednimi danymi np.

real name of tender: piotr;

local email address: piotr@prz.rzeszow.pl;

username for pop3: piotr;

password for pop3: xxx;

- serwer jest już postawiony, ostatnią czynnością jest zastosowanie zmian oraz jego restart;

3. PROTOKOŁY POCZTY

Serwer pocztowy pracuje zazwyczaj jako serwer skrzynki pocztowej, przechowujący pocztę swoich klientów zanim ściągną ją do swoich lokalnych klientów poczty.

Do najbardziej znanych systemów poczty elektronicznej należą:

- protokół SMTP (Simple Mail Transfer Protocol) – internetowy protokół pocztowy zapewniający komunikację z użytkownikami Unixa bez dodatkowych bram
- protokół POP (Post Office Protocol) – aby odebrać przesyłkę pocztową, należy połączyć się z serwerem zawierającym konto pocztowe użytkownika. Zazwyczaj jest ona ściągana do lokalnego komputera. Do ściągania danych służy właśnie protokół POP, pozwala on na wymianę poleceń i potwierdzeń pomiędzy klientem a serwerem poczty.
- protokół IMAP (Internet Message Access Protocol), który staje się ostatnio bardzo popularny

Oprócz podstawowych usług skrzynki pocztowej, systemy linuxowe oferują kilka dodatkowych usług pocztowych, które mogą być przydatne. Jest to m.in. filtrowanie spamu i narzędzia pomagające ograniczyć ilość niepożądanej poczty (tzw. spamu).

Host zmienia się w serwer skrzynki pocztowej, gdy uruchamia demon POP lub IMAP. Większość systemów linuxowych uruchamia oba demony. Żaden z nich nie wymaga konfiguracji. Wszyscy użytkownicy, którzy posiadają konto użytkownika lub konto pocztowe w systemie, mogą ściągać pocztę przez POP lub IMAP.

3.1. Protokół POP

Istnieją dwie wersje protokołu POP: POP2 i POP3. Protokoły te weryfikują nazwę użytkownika i hasło używane przy logowaniu i przenoszą pocztę użytkownika z serwera do lokalnego czytnika poczty na komputerze użytkownika. Oba protokoły wykonują te same podstawowe funkcje, jednakże nie są one kompatybilne. POP2 używa portu 109, a POP3 – portu 110. Systemy linuxowe obsługują obie wersje POP, ale większość klientów używa POP3. Standard protokołu POP3 jest zdefiniowany w dokumencie RFC 1725. Jest to prosty protokół żądanie/odpowiedź: klient wysyła polecenie do serwera, a serwer na nie odpowiada.

Niektóre z poleceń POP3:

- USER nazwa użytkownika – nazwa użytkownika wymagana przy logowaniu
- Pass hasło – hasło użytkownika wymagane przy logowaniu
- STAT – żąda liczby nie przeczytanych wiadomości / bajtów
- RETR m – ściąga wiadomość numer m
- Polecenie – funkcja
- DELE m – kasuje wiadomość numer m
- LAST – żąda numeru ostatniej używanej wiadomości
- LIST [m] – żąda rozmiaru wiadomości m lub wszystkich wiadomości
- RSET – cofa usunięcie wszystkich wiadomości i ustawia numer wiadomości na 1
- TOP m n – drukuje nagłówek i pierwsze n linii wiadomości numer m
- NOOP – niec nie robi
- QUIT – kończy sesję POP3

Dopuszczalne są cztery stany protokołu:

- połączenie (connection) – pierwszy stan po odebraniu nazwy komputera użytkownika wraz z hasłem, po weryfikacji oczekiwana jest odpowiedź „+OK.”
- autoryzacja (authorization) – składa się z wysyłania do serwera POP informacji o użytkowniku i jego haśle po potwierdzeniu hasła przekazywana jest odpowiedź „POP_OK”, po którym wchodzi się w stan transakcji
- transakcja (transaction) – czytanie i usuwanie przesyłek pocztowych
- uaktualnianie (update) – stan końcowy po przekazaniu komendy „QUIT”, w którym uaktualniane są informacje o przeprowadzonej transakcji

3.2. Protokół IMAP

Internet Message Access Protocol (IMAP) jest protokołem warstwy aplikacji w architekturze protokołów Internetowych. Głównym jego zadaniem jest umożliwienie stacji roboczej (np. komputer w domu lub w sieci lokalnej) dostępu do listów elektronicznych znajdujących się w skrzynce pocztowej (mail box) na serwerze pocztowym.

W przeciętnym serwerze POP cała zawartość skrzynki pocztowej jest przesyłana do klienta i albo usuwana z serwera, a albo zatrzymywana tak, jakby nigdy nie była czytana. Usunięcie poszczególnych wiadomości w systemie klienckim nie jest odzwierciedlone w serwerze , ponieważ wszystkie wiadomości są traktowane jako pojedynczy element, który po transferze

danych do klienta albo jest usunięty, albo zatrzymany. IMAP umożliwia manipulowanie poszczególnymi wiadomościami na kliencie lub serwerze w ten sposób, aby zmiany były odzwierciedlane w skrzynkach pocztowych obu systemów.

Podobnie jak POP, IMAP definiuje środki dostępu do listów w skrzynce, a nie środki wysyłania czy transferu listów pomiędzy serwerami pocztowymi. Tą funkcją zajmuje się odpowiedni protokół transferu poczty (np. SMTP - Simple Mail Transfer Protocol). Protokół IMAP zakłada, że ma do dyspozycji wiarygodne medium transmisji strumienia danych, takie jakie przykładowo dostarcza protokół TCP lub jakiś podobny. Gdy używany jest TCP, to program serwera IMAP "nasłuchuje" na porcie 143 czekając na zlecenia. Podsumowując pocztowy protokół dostępu IMAP odzyskuje wiadomości, może modyfikować atrybuty listów; w ogólności zarządza skrzynkami. IMAP oferuje wiele więcej możliwości w stosunku do prostego schematu "skopiuj i usuń" dostępnego w protokole POP.

Protokół IMAP składa się z ciągu komend klienta i odpowiedzi serwera. Dane z serwera przeplatają się z komendami klienta. Inaczej niż ma to miejsce w większości protokołów Internetowych warstwy aplikacji, komendy i odpowiedzi są etykietowane. Serwer (programowy) musi być cały czas gotowy do połączenia. Klient rozpoczyna sesję i oczekuje na "pozdrowienie" z serwera. Generalnie pierwszą komendą klienta jest LOGIN z nazwą konta i hasłem jako parametrami: LOGIN username password. Gdy to się powiedzie, klient musi wysłać komendę SELECT aby dostać się do pożądanej skrzynki. Klient ma możliwość zmieniania pewnych danych, głównie przy pomocy specjalnych flag. Dokonuje się tego komendą STORE. Przykładowo wiadomość pocztowa może być zaznaczona do usunięcia ze skrzynki komendą STORE z ustawioną flagą \DELETED. Inne często używane komendy to: COPY, EXPUNGE, CHECK, SEARCH, LOGOUT. Klient kończy sesję komendą LOGOUT, serwer zwraca BYE i OK.

3.3. Protokół SMTP

Protokół SMTP działa w oparciu o zasadę "magazynuj i przesyłaj dalej" (ang. store-and-forward). Podczas przesyłania może pojawić się wiele pośrednich serwerów MTA, co sprawia, że powiadomienie nadawcy o błędzie spoczywa na każdym z nich.

Wystąpienie ewentualnego problemu wymaga wysłania powiadomienia do nadawcy za pomocą nowej wiadomości - tak zwanej "odbitej" (ang. bounce message). Nadawca takiej wiadomości jest ustawiany na **<>**, aby odbiorca "odbicia" nie mógł na nią odpowiedzieć. Adres ten pojawia się w nagłówku e-maila w polu Return-Path**:**. W polu From: serwer natomiast ustawia adres MAILER-DEAMON@domena.serwera.pl, aby oznaczyć, iż jest to wiadomość od automatu. Treść wiadomości odbitej zależy od konkretnego programu MTA, który ją wygenerował.

Z opisu tego można wyciągnąć prosty wniosek - nie należy wpadać w panikę, gdy zobaczymy w swojej skrzynce pocztowej wiadomość o złowieszczym tytule: Mail delivery subsystem... Zazwyczaj oznacza ona, że jednemu z serwerów MTA uczestniczących w przekazaniu listu nie udało się chwilowo wykonać swojej pracy. Po pewnym czasie podejmie on jednak kolejną próbę.

4. OCHRONA ANTYSPAMOWA

W związku z tym, że poczta elektroniczna (e-mail) jest jedną z najczęściej wykorzystywanych usług dostępnych przez Internet, bardzo ważnym jest ochrona jej zawartości i treści wiadomości otrzymywanych poprzez e-mail. Dostępność i łatwość korzystania z tego rodzaju komunikacji jest używana w wielu przypadkach w sposób niepożądany. Bardzo częstym zjawiskiem jest otrzymywanie tzw. spamu.

Spam (standardowa definicja M.A.P.S.- Mail Abuse Prevention System)

„Elektroniczna wiadomość jest spamem, jeżeli:

(1) treść i kontekst wiadomości są niezależne od tożsamości odbiorcy, ponieważ ta sama treść może być skierowana do wielu innych potencjalnych odbiorców, oraz

(2) jej odbiorca nie wyraził uprzedniej, możliwej do weryfikacji, zamierzonej, wyraźnej i zawsze odwoływalnej zgody na otrzymanie tej wiadomości, oraz

(3) treść wiadomości daje odbiorcy podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z jej odebrania.”

Powyższa definicja została zaczerpnięta ze strony http://lukasz.kozicki.pl/spam/standard.html.

Otrzymywanie spamu jest bardzo uciążliwe zarówno dla użytkownika jak również dla administratora serwera pocztowego. Użytkownik poczty elektronicznej, który otrzymał spam traci czas. Natomiast od strony administratora spamerzy powodują niepotrzebną generację ruchu na łączach do Internetu, gdyż wysyłane przez e-maile z spamem można liczyć co najmniej w setkach.

Walka ze spamerami może się odbywać niejako na dwóch poziomach:

- na poziomie użytkownika,
- na poziomie administratora.

Użytkownik ma do zabezpieczenie przed spamem ma do swej dyspozycji parę możliwości. Po pierwsze filtrowanie wiadomości e-mail w kliencie poczty wykorzystywanym na swoim komputerze. Ustawienie odpowiednich opcji zależy od danego programu. Druga możliwość to korzystanie z konta shellowego (np. linux’owego) z dostępem do procmail’a. Procmail jest bardzo użytecznym narzędziem służącym do filtracji otrzymywanej poczty elektronicznej. Głównym plikiem służącym do ustawień filtra antyspamowego jest plik .procmailrc. Plik ten musi się składać z odpowiednich wpisów spełniających następujące kryteria:

0 oznacza początek polecenia, to występuje zawsze na początku.

^ oznacza początek linii

. oznacza dowolny znak

.+ oznacza dowolny ciąg znaków (ale co najmniej jeden),

.* oznacza dowolny ciąg znaków (także ciąg pusty znaków...)

* oznacza zero lub więcej powtorzeń wyrażenia który jest przed "gwiazdką" / dowolny ciąg znaków

$ oznacza koniec linii

{} otwarcie i zamknięcie bloku danych.

de|abc oznacza sekwencję znaków `de' lub `abc' (alternatywa).

a* oznacza dowolną sekwencję z a na początku (jedno i więcej)

(abc)* sekwencja abc powtarza się zero lub kilka razy (dowolna ilosć powtorzeń)

Przykładowo więc następujący zapis:

```
:0
* ^From:.*@poczta.onet.pl
/dev/null
```

oznacza usunięcie wszelkich przesyłek z jakiegokolwiek konta z poczta.onet.pl.

Zablokowanie natomiast wszelkich przesyłek, które nie będą miały naszego adresu (np.: moj_adres@np_poczta.pl) w polu TO: uzyskamy dzięki następującemu wpisowi:

```
:0
* ^TO: .*mój_adres@np_poczta.pl
/dev/null
```

Innym istotnym działaniem związanym z zabezpieczeniem przed spamem jest ochrona własnego adresu e-mail i nie udostępnianie go na „forum publicznym" tzn. np.: na stronach internetowych (mailto:adres@poczta.pl), w wiadomościach do grup dyskusyjnych, itp. Takie działania są koniecznością, aby uchronić własną skrzynkę przez wykrycie adresu przez programy przeszukujące np.:strony WWW pod kątem adresów, czyli słów „mailto", „@",itp. Często stosowane są stosowane zabezpieczenia w postaci umieszczania w adresie e-mailowym słów, które się tam w rzeczywistości nie znajdują, a które mogą być usunięte przez człowieka, natomiast rzadziej przez program np.: moj_adresNOSPAM@poczta.pl lub moj_adresUSUN_TO@poczta.pl, itp.

W walce ze spamerami istotną sprawą jest postawa administratorów serwerów poczty jak również prowiderów internetowych. Ponieważ zablokowanie, na serwerach, adresów internetowych, a nawet adresów IP, z których wysyłany jest spam daje dużo lepsze efekty i dodatkowo zmniejsza ruch w sieci.

Dlatego tez powstają organizacje zajmujące się zbieraniem danych o spamerach oraz udostępnianie tych informacji wszystkim zainteresowanym (np.: SpamCop, abuse.net, PolSpam). Współpraca z takimi organizacjami zwiększa szanse szybkiego zablokowania spamu. Do PolSpamu zgłaszać się mogą zarówno użytkownicy otrzymujący spam jak i administratorzy serwerów pocztowych. Zgłoszenie spamu może nastąpić przez formularz na stronie WWW (www.polspam.org/report.php) lub przez e-mail poprzez przesłanie otrzymanej wiadomości ze spamem (jako załącznik) na adres abuse@polspam.org.

Administratorzy serwerów pocztowych mogą natomiast pobierać bazę danych spamerów zapisaną w PolSpam, oraz dołączać ją do lokalnej bazy danych spamerów na swoich serwerach. Aktualizacja bazy danych może odbywać poprzez stronę WWW PolSpamu, przez listę mailingową lub z wykorzystaniem odpowiednich skryptów.

5. OCHRONA ANTYWIRUSOWA

Ochrona antywirusowa serwerów pocztowych stała się niezbędna w ostatnich czasach, gdyż coraz więcej wirusów rozprzestrzenia się poprzez pocztę elektroniczną.

Najprostszym sposobem ochrony antywirusowej jest instalacja odpowiedniego oprogramowania wykrywającego wirusy.

Obecnie jest wiele firm oferujący skanery antywirusowe, zarówno na platformę Windows jaki i dla systemów UNIX'owych. Zwykle program taki wystarczy zainstalować, odpowiednio skonfigurować i uruchomić. Istotnym jest jednak możliwość odświeżanie bazy danych wirusów rozpoznawanych przez dany program. Większość jednak producentów oprogramowanie umożliwia taką operację poprzez Internet.

Drugim sposobem na ochronę antywirusową może być wykorzystanie programu procmail. Można bowiem ustawić w nim odpowiednie warunki usuwające zawirusowaną pocztę, np.: poprzez usunięcie wiadomości zawierających w tytule wyrażenie from.my.party! (używanego

przez robaka W32/Myparty-mm)
:0
* ^Subject:.*from.my.party!
null/dev

Rozwiązanie takie wymaga stałej kontroli pojawiania się nowych wirusów, a także wiedzy na temat stałych elementów znajdujących się w zainfekowanych wiadomościach pocztowych.

LITERATURA

http://lukasz.kozicki.pl/spam/standard.html
http://republika.pl/fuckspam/procmail.html
http://www.polspam.org/
Chip – sierpień 2002