

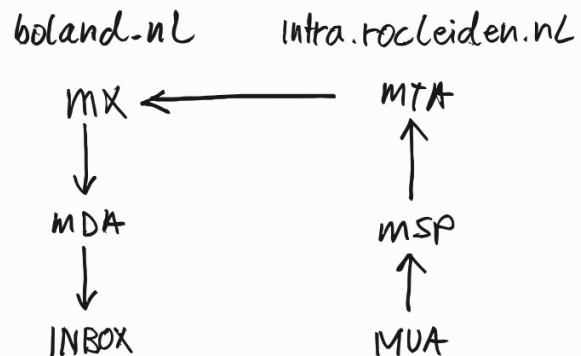
Huiswerk Linux: Sendmail Ring of Trust

In de vorige opdracht hebben we een e-mail naar een andere gebruiker op hetzelfde systeem verzonden. Dit was in de tijd van de mainframes voldoende. Alle gebruikers binnen de instelling werkten op dezelfde computer. De volgende stap was het versturen van e-mail naar *andere* computers (hosts) in het netwerk.

De opdracht voor deze week is: zoek de Mail Exchangers voor de volgende e-mail adressen op: d.boland@rocleiden.nl, daniel@boland.nl, daniel.boland@student.rocleiden.nl

Over het Ring of Trust model

Zoals je weet is het Internet voor een groot deel mogelijk gemaakt door hippies. Hippies houden niet van autoriteit en centraal gestuurde maatschappijen. Zij houden niet van wachtwoorden, zij houden niet van encryptie. Daarom hebben zij hard en lang nagedacht hoe je een elektronische maatschappij decentraal bestuurt. Dit valt allemaal onder het begrip *internet governance*. Eén van de geniale oplossingen die zijn verzonden is het *Ring of Trust* model.



Het *Ring of Trust* model is een alternatief op het gebruik van wachtwoorden om e-mail van de ene naar de andere computer te verplaatsen. In plaats van wachtwoordcontrole wordt gekeken naar de afzender en het domein van waaruit de e-mail verstuurd is.

Over E-Mail routing

Het *Ring of Trust* model werkt, net als bij *IP-routing*, met subnets. Het verschil met TCP/IP is dat *e-mail routing* geen IP-adressen gebruikt, maar domeinnamen. Als je dus een e-mail wilt versturen naar iemand die zich buiten jouw subnet (domein) bevindt, dan moet de e-mail via een router verstuurd worden. Deze router wordt in de mail-wereld de *Mail Exchanger* (MX) genoemd.

Mail User Agent (MUA)

De e-mail wordt samengesteld in een *Mail User Agent* (MUA). Dit is meestal een programma waarmee de gebruiker ook haar e-mail leest. Voorbeelden zijn: *mail*, *mutt*, *MS Outlook Express*, *Netscape Mail*, *Mozilla Thunderbird*, *NextMail*, *AppleMail*, *Windows Live Mail*. De ongeformatteerde e-mail-tekst wordt via een *pijpleiding* aangeboden aan het *Message Submission Program*.

Message Submission Program (MSP)

Het *Message Submission Program* (MSP) zorgt ervoor dat de e-mail het juiste format krijgt. In de Windows varianten is deze functionaliteit reeds ingebouwd in de *MUA*, maar onder Linux worden hier afzonderlijke programma's voor gebruikt. Voorbeelden zijn: *mail*, *sendmail*, *exim*, *postfix*, *MAPI* en *QMail*. Het format bestaat uit drie *MIME headers* en ziet er ongeveer als volgt uit:

```
Return-Path: <daniel@dimension.intra.rocleiden.nl>
Received: (from daniel@smtp.boland.nl)
    by dimension.intra.rocleiden.nl (8.14.9/8.14.9/Submit) id s8K62Wc0000760
    for daniel@smtp.boland.nl; Sat, 20 Sep 2014 08:02:32 +0200
Message-Id: <201409200602.s8K62Wc0000760@dimension.intra.rocleiden.nl>
```

De geformatteerde e-mail wordt vervolgens aangeboden (*submitted*) aan de *Mail Transfer Agent*.

Mail Transfer Agent (MTA)

De *Mail Transfer Agent* (MTA) is een *daemon*: een programma dat in de achtergrond luistert naar connecties op poort 25. Voorbeelden van MTA-programma's zijn: *MS Exchange*, *Sendmail* en *QMail*. De MTA daemon controleert of de afzender- en ontvanger-adressen geldig zijn en voegt de volgende *MIME header* toe:

```
Received: from dimension.intra.rocleiden.nl (localhost [127.0.0.1])
        by dimension.intra.rocleiden.nl (8.14.9/8.14.9) with ESMTTP id s8K62XrK001056
        for <daniel@smtp.boland.nl>; Sat, 20 Sep 2014 08:02:33 +0200
```

Indien de geadresseerde zich op dezelfde (lokale) computer bevindt, biedt de MTA daemon de e-mail rechtstreeks aan bij de lokale *Mail Delivery Agent*, welke de e-mail in de *INBOX* van de ontvanger plaatst.

Indien de geadresseerde zich *niet* op dezelfde computer bevindt, zoekt de MTA daemon de naam van de computer op, waar de ontvanger haar *INBOX* heeft en biedt de e-mail aan bij de *Mail Exchanger* van die computer.

Mail Exchanger (MX)

De *Mail Exchanger* (MX) is ook een *daemon*: hij luistert op poort 25 naar binnenkomende connecties van *Mail Transfer Agents*. Voorbeelden van MX-software zijn: *MS Exchange*, *Sendmail* en *QMail*. Ook de MX daemon controleert of de afzender- en ontvanger-adressen geldig zijn en voegt de volgende *MIME header* toe:

```
Received: from dimension.intra.rocleiden.nl (boland.xs4all.nl [213.84.69.3])
        by smtp.boland.nl (8.14.0/8.14.0) with ESMTTP id s8KAGld3023872
        for <daniel@smtp.boland.nl>; Sat, 20 Sep 2014 12:16:47 +0200 (CEST)
```

De betekenis van deze regel (*header*) is als volgt: de computer, genaamd *smtp* heeft van een computer, genaamd *dimension*, een e-mail ontvangen voor gebruiker *daniel*. Ook kunnen we zien hoe de **Ring of Trust** werkt. De MX-daemon heeft een *reverse lookup* op de verzendende computer uitgevoerd. Het resultaat zie je tussen haakjes staan (*boland.xs4all.nl [213.84.69.3]*). Dit is een geheel andere naam dan de naam waarmee de computer zichzelf bekend maakt (*dimension.intra.rocleiden.nl*). Voor veel MX-daemons is dit een reden om de e-mail te weigeren.

Indien de geadresseerde zich niet op de lokale computer bevindt, weigert de MX-daemon de e-mail te ontvangen met de foutmelding: *We do not relay*. Hier komen we later nog op terug.

Indien de geadresseerde zich wél op de lokale computer bevindt biedt de MX daemon de e-mail via een *pijpleiding* aan bij de *Mail Delivery Agent*.

Mail Delivery Agent (MDA)

De *Mail Delivery Agent* (MDA) ontvangt e-mail welke geadresseerd is aan gebruikers van de lokale computer. Het MDA programma plaatst de e-mail in de **INBOX** map van de betreffende gebruiker. Voorbeelden van MDA software zijn: *mail*, *deliver*, *maildrop*, *Cyrus IMAP*, *Dovecot* en *procmail*.

Het *sudo* mechanisme

Het installeren van nieuwe software doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator.

Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Het *dig* programma is onderdeel van het *bind-utils* pakket. We gaan dit installeren via het *apt-get* programma:

apt-get install bind-utils

Zorg er ook voor dat de Sendmail daemon is gestart:

service sendmail start

Andere Linux gebruikers

Sudo voor gebruikers van andere Linux-versies (*Ubuntu, Lubuntu, Kubuntu, OSX, Android, Gentoo, Debian*, etc): start een terminal met de toetsencombinatie **<Ctrl><Alt>-T**. We gebruiken het commando *sudo* om in te loggen met het *su* (become Super User) commando. Daardoor blijven we ingelogd:

sudo su

Het *dig* programma is onderdeel van het *bind-utils* pakket. We gaan dit installeren via het *apt-get* programma:

apt-get install dnsutils

Zelf mail exchangers opzoeken

Zoals in de vorige paragraaf beschreven is Sendmail een *Mail Transfer Agent* (MTA) en dus in staat om zelf de computers te vinden waar de e-mail uiteindelijk naartoe moet. Daarvoor gebruikt Sendmail het *Domain Name System* (DNS). Om te zien hoe dit werkt gaan we zelf het DNS raadplegen.

Opzoeken rocleiden.nl

Het eerste adres dat we opzoeken is `d.boland@rocleiden.nl`. Het e-mail adres is als volgt opgebouwd:

gebruikersnaam	op	hostnaam
d.boland	@	rocleiden.nl

Om erachter te komen waar de e-mail voor deze gebruiker naartoe moet, gaan we opzoeken hoe de MX-daemon van het domein heet. Dit doen we met het zoëven geïnstalleerde *dig* (Domain Information Groper) programma:

dig rocleiden.nl mx

Via de eerste parameter geven we aan dat we informatie willen opvragen van het domein *rocleiden.nl*. Via de tweede parameter geven we aan dat we de *MX* regel (*record*) willen opvragen. De output ziet er als volgt uit:

```
; <<>> DiG 9.9.5 <<>> rocleiden.nl mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9240
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rocleiden.nl.                IN      MX

;; ANSWER SECTION:
rocleiden.nl.                20800  IN      MX      10 mx-a.mf.surf.net.
rocleiden.nl.                20800  IN      MX      10 mx-1.mf.surf.net.

;; AUTHORITY SECTION:
rocleiden.nl.                7200   IN      NS      ns1.zurich.surf.net.
rocleiden.nl.                7200   IN      NS      ns1.surfnet.nl.
rocleiden.nl.                7200   IN      NS      ns2.surfnet.nl.
rocleiden.nl.                7200   IN      NS      ns3.surfnet.nl.

;; ADDITIONAL SECTION:
ns1.zurich.surf.net.        120849 IN      AAAA    2001:620:0:9::1103
ns1.surfnet.nl.            7200   IN      A       192.87.106.101
ns1.surfnet.nl.            7200   IN      AAAA    2001:610:1:800a:192:87:106:101
```

```

ns2.surfnet.nl.      7200    IN      A       192.87.36.2
ns2.surfnet.nl.      7200    IN      AAAA    2001:610:3:200a:192:87:36:2
ns3.surfnet.nl.      7200    IN      A       195.169.124.71
ns3.surfnet.nl.      7200    IN      AAAA    2001:610:0:800c:195:169:124:71

```

In de **QUESTION** sectie staat de gestelde vraag: geef ons het MX record van het domein *rocleiden.nl*. In de **ANSWER** sectie zien we dat er twee records gevonden zijn: *mx-a.mf.surf.net* en *mx-1.mf.surf.net*. De getallen ervoor (*10* en *10*) geven de prioriteit aan waarmee de servers gebruikt moeten worden.

In de **AUTHORITY** sectie zien we welke DNS servers verantwoordelijk zijn voor het bijhouden van de DNS records van het domein *rocleiden.nl*. In de **ADDITIONAL** sectie kunnen we zien wat de IP-adressen van deze DNS-servers zijn.

Opzoeken boland.nl

Het volgende adres dat we opzoeken is mijn privé adres: *daniel@boland.nl*. Het e-mail adres is als volgt opgebouwd:

gebruikersnaam	op	hostnaam
daniel	@	boland.nl

Om het MX record van mijn domein op te zoeken, kunnen we ook het *nslookup* programma gebruiken:

```
nslookup -type=mx boland.nl
```

Via optie *type* geven we aan dat we het *record* (regel) van het type *MX* willen opvragen. Zoals je ziet is de output een stuk korter:

```

Server:      10.0.0.200
Address:     10.0.0.200#53

boland.nl    mail exchanger = 5 mail.boland.nl.

```

Opdracht

Zoek nu zelf de *Mail Exchanger* van jouw student-mail adres (*xxx.xxx@student.rocleiden.nl*) op. Stuur je antwoord op via het huiswerksysteem. Dit doe je met een pijpleiding tussen de commando's *echo* en *email*. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
echo "ANTWOORD" | email -s "MX opzoeken" docent@localhost
```

Let op: vervang *ANTWOORD* door de mail exchanger die jij gevonden hebt. Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben de *mutt* e-mail client geïnstalleerd en zelf Mail Exchangers opgezocht, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.