Huiswerk Linux: Instellen *reverse lookup zone*

Het tweede wat je moet doen als je een eigen DNS in gebruik neemt is het instellen van *reverse lookups* van je eigen *Local Area Network* (LAN). Dit zorgt ervoor dat de verschillende servers in je netwerk elkaar vertrouwen. De opdracht voor deze week is: voeg de *reverse lookup zone* van je eigen *Local Area Network* (LAN) aan het domeinnaamsysteem (DNS) toe.

Over *reverse lookup zones*

Reverse lookups (FQDN opzoeken via een IP-adres) worden vaak niet ingesteld op DNS systemen, maar ze zijn belangrijk voor zogenaamde *trusted connections* (zie ook: Linux opdracht *Ring of Trust*). Servers die vertrouwelijke informatie verwerken zoals wachtwoorden, willen weten of de client-computer wel in hun netwerk thuishoort. Dit doen ze door het IP-adres te gebruiken om de *fully qualified domain name* (FQDN) van de client-computer te controleren.

Het instellen van een *reverse lookup zone* is wat ingewikkelder dan gewone *forward lookup zones* uit de vorige opdracht. Stel, je wilt een reverse lookup zone aanmaken voor de volgende machine:

FQDN: dimension.testdomein.dmz
IP-adres: 192.168.137.50
Netmask: 255.255.255.0

Het netmasker bepaalt welk deel van het IP-adres de *zone* en welk deel de *node* is. De bovenstaande gevens zien er dan alsvolgt uit. Zoals je ziet bestaat de combinatie van zone en node uit de **omgekeerde getallen** van het bovenstaande IP-adres:

```
50.137.168.192.in-addr.arpa
-node-   -zone-------------------------------------------------------------
```

Het *sudo* mechanisme

Het configureren van Linux doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator (root).

Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Zorg er ook voor dat je DNS-server draait. Dit doe je met het *service* programma:

```
service bind start
```

Andere Linux gebruikers

Sudo voor gebruikers van andere Linux-versies (*Ubuntu*, *Lubuntu*, *Android*, *Debian, UberStudent*, 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
```

Zone-bestand aanmaken

Net als in de vorige opdracht gaat het toevoegen van *reverse lookup records* in twee stappen: het aanmaken van de *reverse lookup zone* en het toevoegen van de zone aan het configuratiebestand van de BIND name-server.

Cygwin gebruikers

In een Cygwin distributie staan de zone-bestanden in de directory */var/named*. Zorg ervoor dat je in die directory staat:

```
cd /var/named/master
```

Andere Linux gebruikers

Bij andere Linux-versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) staan de zone-bestanden in de */var/cache* directory. Zorg ervoor dat je in die directory staat:

```
cd /var/cache/bind/master
```

Iedere zone krijgt een eigen bestand, net als bij de configuratie van Apache (zie: *Apache Includes*). We maken het bestand aan met de *vi* editor:

```
vi 137.168.192.in-addr.arpa
```

Je ziet een leeg scherm. Toets **i** (insert) om naar de *INSERT* modus te gaan en voeg de volgende regels toe:

```
@            IN  SOA   dimension.testdomein.dmz. hostmaster (
                       2010011201; serial
                       86400; refresh
                       1800; retry
                       1209600; expire
                       43200; default_ttl
                       )
@            IN  NS    ns1.testdomein.dmz.
1            IN  PTR   dimension.testdomein.dmz.
```

Let op: *dimension* is de hostnaam van mijn machine. Gebruik hier de hostnaam van jouw eigen machine. Als je deze niet weet, zoek hem dan op met het commando *hostname*.

Het **SOA (Start Of Authority) record** geeft aan wie verantwoordelijk is voor het bijhouden van de zone en begint altijd met een @ (at) teken. Dit teken wordt door de server vervangen door de zone welke we willen toevoegen, in dit geval *137.168.192.in-addr.arpa*. De letters *IN* (internet) geven aan om welk soort zone het gaat.

Een **NS (Nameserver) record** begint ook altijd met een @ (at) teken en geeft aan op welke machine we het zone-bestand kunnen vinden.

Een **PTR (Pointer) record** begint altijd met het unieke node-nummer van een machine en vormt hierdoor een terugverwijzing (pointer) naar de FQDN van die machine.

Toets **<Esc>** om de *INSERT* modus te verlaten en geef de *vi* commando's *w* (write) en *q* (quit):

```
:wq
```

Het zone-bestand wordt opgeslagen en we zijn terug op de Linux command-line.

DNS configureren

Om ervoor te zorgen dat de BIND Name daemon het bovenstaande zone-bestand kan vinden, moeten we het toevoegen aan het *named.conf* configuratie-bestand.

Cygwin gebruikers

Open het configuratiebestand met de *vi* editor:

```
vi /etc/named.conf
```

Andere Linux gebruikers

Bij andere Linux-versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) staat het bestand in de */etc/bind* directory:

```
vi /etc/bind/named.conf.local
```

Dit bestand ziet er op iedere Linux distributie anders uit, maar de instellingen zijn hetzelfde. Ga naar het einde van het bestand met (hoofdletter) **G**. Toets **i** (insert) om naar de *INSERT* modus te gaan en voeg de vetgedrukte regels toe:

```
zone "testdomein.dmz" {
        type master;
        file "master/testdomein.dmz";
};
zone "137.168.192.in-addr.arpa" {
         type master;
         file "master/137.168.192.in-addr.arpa";
};
```

Toets **<Esc>** om de *INSERT* modus te verlaten en geef de *vi* commando's *w* (write) en *q* (quit):

```
:wq
```

Het configuratiebestand wordt opgeslagen en we zijn terug op de Linux command-line.

Het hoera-moment

Allereerst moeten we ervoor zorgen dat de BIND name daemon de gewijzigde instellingen opnieuw inleest. Dit doen we door BIND te herstarten met het *service* programma:

```
service bind restart
```

Let op: in andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc.) heet de service **bind9**.

Nu kunnen we de configuratie van de *reverse lookup zone* testen. Dit doen we door een zogenaamde *reverse lookup query* op één van de machines in de zone uit te voeren. Dit doen we met het progamma *nslookup*:

```
nslookup 192.168.137.1
```

De output moet er alsvolgt uitzien. Als het goed is staat achter de veldnaam *Server* het IP-adres van de localhost (127.0.0.1). Dit betekent dat de query via je eigen DNS is uitgevoerd:

```
Server:         127.0.0.1
Address:        127.0.0.1#53

1.137.168.192.in-addr.arpa      name = dimension.testdomein.dmz.
```

Let op: *dimension* is de host-naam van mijn machine. Je moet hier jouw eigen host-naam kunnen zien.

Huiswerk opsturen

Je kunt de opdracht aftekenen door mij een e-mail met de output van het bovenstaande *nslookup* commando te sturen. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
nslookup 192.168.137.1 | email -s "BIND reverse lookup" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben een *reverse lookup zone* aan de BIND DNS server toegevoegd en getest, maar we zijn nog steeds ingelogd als Administrator (*root*).

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

Problemen oplossen

Als je hier een foutmelding krijgt, kijk dan in het algemene logbestand van Linux. Hier worden eventuele foutmeldingen bijgeschreven:

```
tail /var/log/daemon
```

Let op: in sommige Linux systemen heet het algemene logbestand **/var/log/daemon.log**. De output van een correct geïnstalleerde DNS server ziet er ongeveer alsvolgt uit:

```
Apr 17 20:20:10 optiplex named: PID 2644: starting BIND 9.10.2 -u named -f
Apr 17 20:20:10 optiplex named: PID 2644: built with '--prefix=/usr' '--localstatedir=/var' '--with-
     randomdev=/dev/urandom' '--disable-static' 'CC=gcc' 'CFLAGS=-DFD_SETSIZE=256' 'LDFLAGS='
     'LIBS=/lib/libfakesu.a' 'CPPFLAGS='
Apr 17 20:20:10 optiplex named: PID 2644: ------------------------------------------------------
Apr 17 20:20:10 optiplex named: PID 2644: BIND 9 is maintained by Internet Systems Consortium,
Apr 17 20:20:10 optiplex named: PID 2644: Inc. (ISC), a non-profit 501(c)(3) public-benefit
Apr 17 20:20:10 optiplex named: PID 2644: corporation.  Support and training for BIND 9 are
Apr 17 20:20:10 optiplex named: PID 2644: available at https://www.isc.org/support
Apr 17 20:20:10 optiplex named: PID 2644: ------------------------------------------------------
Apr 17 20:20:12 optiplex named: PID 2644: command channel listening on 127.0.0.1#953
Apr 17 20:20:12 optiplex named: PID 2644: all zones loaded
Apr 17 20:20:12 optiplex named: PID 2644: running
```