Arquitetura de Redes

Laboratory Guide

Objectives

- Study of the DNS and DNSSEC

Consider a PC and a Server in the same network (10.1.1.0/24). The server used in this guide is a bare installation of the Ubuntu 12.04 Server.

DNS

1. Configure your terminal (Linux) with the IP address 10.1.1.201/24. Test the connectivity with your server (using the command ping) which should have the IP address 10.1.1.21. Connect to your server (which is running Linux) using SSH (login: *root*, password: *labcom*). The server is running a DNS server (bind9) with default configuration.

2. Assuming that you own the domain **grupo1ar.com** configure your DNS server to act as a master server (zone) for that domain. Start by creating the definition of the zone with the associated *statements* (zone specific parameters), edit the file /etc/bind/named.conf.local (with root privileges) and add the following definition:

```
zone "grupo1ar.com" in{
   type master;                  //statement to define the zone as master
   file "/etc/bind/db.grupo1ar.com";          //location of the zone file with the records
};
```

Create the file /etc/bind/db.grupo1ar.com (with root privileges) and add the following contents:

```
$TTL   604800
$ORIGIN grupo1ar.com.
@      IN     SOA    ns1.grupo1ar.com. adm.grupo1ar.com. (
                          2             ; Serial
                     604800             ; Refresh
                      86400             ; Retry
                    2419200             ; Expire
                     604800 )     ; Negative Cache TTL
       IN     NS     ns1.grupo1ar.com.
       IN     A      10.1.0.1
       IN     AAAA   2001:A:0::1
       IN     MX     10     server1
ns1    IN     A      10.1.0.1
server1       IN     A      10.1.0.2
server2 IN    CNAME  server1
```

Verify if your zone file it is correctly defined:

```
named-checkzone grupo1ar.com db.grupo1ar.com
```

Restart your DNS server:

```
service bind9 restart
```

Using your PC, test the configuration of your DNS by performing the following DNS queries:

```
dig @10.1.1.21 grupo1ar.com
dig @10.1.1.21 grupo1ar.com AAAA
dig @10.1.1.21 server1.grupo1ar.com
dig @10.1.1.21 server2.grupo1ar.com
dig @10.1.1.21 grupo1ar.com MX
```

Analyze the output of the dig commands.

3. Add a zone to configure the IPv4 reverse DNS mapping of your domain. Add to /etc/bind/named.conf.local the following zone definition:

```
zone "0.1.10.in-addr.arpa" in{
  type master;
  file "/etc/bind/db.10.1.0.rev";
};
```

Create the file /etc/bind/db.10.1.0.rev (with root privileges) and add the following contents:

```
$TTL   604800
$ORIGIN 0.1.10.in-addr.arpa.
@      IN     SOA    ns1.grupo1ar.com. adm.grupo1ar.com. (
                          2             ; Serial
                     604800             ; Refresh
                      86400             ; Retry
                    2419200             ; Expire
                     604800 )     ; Negative Cache TTL
              IN      NS      ns1.grupo1ar.com.
1             IN      PTR     server1.grupo1ar.com. ; qualified name
2             IN      PTR     server2.grupo1ar.com.
```

Restart your DNS server:

```
 service bind9 restart
```

Using your PC, test your configuration with the commands:

```
 nslookup 10.1.0.1 - 10.1.1.21
 nslookup 10.1.0.2 - 10.1.1.21
```

4. Add the necessary DNS records to the configuration of your master DNS server considering that your network has:

- A new (backup) e-mail server.
- A new HTTP webmail interface (in the main e-mail server) accessible by IPv4 and IPv6 using the sub-domains: webmail.grupo1ar.com or mail.grupo1ar.com.
- A new (slave) DNS server with the name ns2.grupo1ar.com (you don't have to define the slave zone, just the necessary records in the master zone).
- A new DNS server (with the name ns3.machines.grupo1ar.com) to handle all names with the sub-domain machines.grupo1ar.com.

Using your PC, test the new configurations using the command dig.

DNSSEC

5. Add DNSSEC configuration to your domain name zone (defined in 2). Start by generating the ZSK public and private keys:

```
dnssec-keygen -a RSASHA1 -b 512 -n ZONE grupo1ar.com
```

And, the KSK public and private keys:

```
dnssec-keygen -a RSASHA1 -b 512 -n ZONE -f KSK grupo1ar.com
```

Note: The size of the keys are smaller that recommended to expedite the creation of the keys. Also, if the generation of the keys gets to long use the option -r /dev/urandom. This option is not recommended in real scenarios because it generates keys with very low entropy.

Open the generated files (Kgrupo1ar.com+005+*.key and Kgrupo1ar.com+005+*.private) and analyze the contents of the public and private keys. Include **both public** keys into your zone file:

```
cat Kgrupo1ar.com+005+*.key >> db.grupo1ar.com
```

Verify the contents of your zone file (`cat db.grupo1ar.com`).

Sign your zone file with the following command:

```
dnssec-signzone -g -l dlv.isc.org -o grupo1ar.com -N INCREMENT db.grupo1ar.com
```

Verify and analyze the contents of your: (i) signed zone file (`cat db.grupo1ar.com.signed`), (ii) DS records file (`cat dsset-grupo1ar.com`) and (iii) DLV records file (`cat dlvset-grupo1ar.com`).

6. Using your PC, connect to the Internet using the wireless network. Verify if the command `drill` is available, if not, install the package *ldnsutils* with the command:

```
sudo apt-get install ldnsutils
```

With Wireshark start a packet capture, and execute the following command:

```
drill -T -D paypal.com @8.8.8.8
```

Try to interpret the command output and the captured packets (DNS queries and answers).