Lab Exercise 5 – Authoritative DNS Servers (IPv6 Reverse DNS Zone Configuration)

Objectives

In this lab, the participants are going to configure the reverse dns zones for their given IPv4 and IPv6 prefixes. They would also configure secondary name server to do a zone transfer between the primary and secondary. This should include creating PRT records. The reverse dns delegations for the IPv4 and IPv6 prefixes of each group/participant have already been done from the in-addr.arpa and ip6.arpa zone. A custom lab root hint will be used.

*Note: Configure your PC to be the primary (also called master) of your own domain and also a slave for PCs in your right side. PC in your left will act as slave for your own domain. *

Steps:

1. Check the delegated IPv4 and IPv6 prefixes for each group. It should be something link 10.0.XX.0/24 for IPv4 and 2001:db8:XX::/48 for IPv6 where XX is your group number. For example, group5 has 10.0.5.0/24 and 2001:db8:5::/48 for reverse dns delegation in this lab.

2. Create a new zone file under `/etc/bind/zones` and add necessary resource records like NS record and PTR record.

   For groupXX, you need to create `db.XX.db8.2001.ip6.arpa`, with the following base contents:

```
$TTL 1d
;; $ORIGIN 0.0.0.0.XX.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

@   SOA     ns.groupXX.net. email.groupXX.net.   (
         2022040601 ;serial no.
         30m        ;refresh
         15m        ;retry
         1d         ;expire
         30m        ;negative cache ttl
        )

            NS      ns.groupXX.net.

;; Reverse DNS records

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR ns.group1.com.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR www.group1.com.
```

3. Add the zone to the configuration file (`named.conf.local`) as done for the forwarding DNS.

```
zone "0.0.0.0.XX.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
    type master;
    file "/etc/bind/zones/db.XX.db8.2001.ip6.arpa";
};
```

4. Change the owner to `bind` for the files in `/etc/bind/zones`

```
sudo chown -R bind:bind /etc/bind/zones
```

5. Check for any syntax errors in the config files or in the zone files.

```
 named-checkconf
 named-checkzone 0.0.0.0.XX.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
/etc/bind/zones/db.XX.db8.2001.ip6.arpa
```

6. Try running bind with -g and -c named.conf and see if BIND complains for errors. Use either:

```
 sudo systemctl restart bind9
```

or

```
 named -g -c named.conf -u bind
```

or

```
 rndc reconfig
```

7. There are couple of commands to check BIND service and logs:

```
sudo systemctl status bind9
```

or

```
sudo tail -f /var/log/syslog
```

or

```
rndc status
```

8. Once BIND is running, you can do some basic test using DNS tools like `dig`

   To test your name server to display the SOA records for your domain.

```
dig -x @localhost 2001:db8:XX::2
```

9. Setup your server as the secondary server for your neighbour.

   In your `named.conf.local`, add the following (groupYY.net is the neighbour zone):

```
zone "0.0.0.0.YY.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
    type slave;
    file "/etc/bind/zones/db.YY.db8.2001.ip6.arpa";
    masters { 10.0.YY.1; 2001:db8:YY::1;
    };
};
```

10. Secure your zones by restricting who can get the zone file.
    You can test this by trying zone transfer from another nameserver in the lab.

```
dig @localhost 0.0.0.0.YY.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa AXFR
```

    If successful, you will see all the resource records as an output.

    Now, add the following line in your `named.conf.local` for the zones where you are primary:

```
zone "0.0.0.0.XX.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
    type master;
    file "/etc/bind/zones/db.XX.db8.2001.ip6.arpa";
};
    allow-transfer { 10.0.YY.1; 2001:db8:YY::1;
    };
};
```

    Execute the same dig command again. If NOT successful, the status in the dig output should say Transfer Failed.

11. You can make `ns.groupYY.net.` (the secondary/slave server) as authorative server. For that add another NS record in the `db.XX.db8.2001.ip6.arpa` file:

```
$TTL 1d
;; $ORIGIN 0.0.0.0.XX.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

@   SOA     ns.groupXX.net. email.groupXX.net.   (
         2016010101 ;serial no.

<config sniff..........>

            IN  NS   ns.groupXX.net.
            IN  NS   ns.groupYY.net.

<config sniff.........>
```

Lab Exercise 5 – Authoritative DNS Servers (IPv6 Reverse DNS Zone Configuration) Created: 12 May 2016 Version 3.1