Lab Exercise 6 – TSIG for Secure Zone Transfer

Objective:
Be able to secure zone transfer between master & slave name server using TSIG keys.

Steps:

1. All the master server will derive a key using "dnssec-keygen" statement

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST <ns1-ns2.mydomain.net>
```

   Check that this generates two files
   ls -al
   K<ns1-ns2.mydomain>.+157+<XXXXX>.key
   K<ns1-ns2.mydomain>.+157+<XXXXX>.private

   Note: Make sure that the key name is as descriptive as possible. In our example, the name chosen is ns1-ns2.mydomain.net to show that it is for the domain mydomain.net and the TSIG key is to be exchanged between ns1 (the primary server) and ns2 (the secondary server).

2. Update the primary server's named.conf with this key. It is recommended to put it in a separate file and use the "include" statement in named.conf to specify this key.

   1. Copy the key part into a file and name it ns1-ns2.mydomain.key. The format is as follows:

```
key ns1-ns2.mydomain {
      algorithm HMAC-MD5;
      secret "<copy-the-secret-here>";
};
```

   2. Edit named.conf and add the #include statement.

```
include "ns1-ns2.mydomain";
server <ip-of-slave> {
      keys { ns1-ns2.mydomain; };
};
```

   3. Now edit named.conf to allow zone transfer from slave servers with the generated key instead of IP addresses.

```
allow-transfer {
      //192.168.102.1   (comment this out)
      key ns1-ns2.mydomain;  //use keys for secure zone transfer
};
```

3. Send the key off-band to your slave name server administrator so they could configure their slave name server to use the key. To do this,

   a. Copy the key to the slave server securely.

```
scp <ns1-ns2.mydomain.key> nsadmin@<ip-address-of-slave-
server>:/var/named/master/
```

Ex: for server1

```
scp ns1-ns2.mydomain.key nsadmin@192.168.102.1:/var/named/master
```

b. Update the secondary server's named.conf to reflect the same changes as the primary.

```
include "ns1-ns2.mydomain";
server <ip-of-master> {
   keys { ns1-ns2.mydomain; };
};

allow-transfer {
//192.168.102.1     (comment this out)
key ns1-ns2.mydomain;     //use keys for secure zone transfer
};
```

4. Run both master & slave nameserver and see if zone transfers happen. Zone transfer can also be tested using dig command, try using it with a key.

Example: Without the key, transfer is expected to fail.

```
dig @server domain axfr

Result:
Transfer failed.
```

Example: with a key

```
dig @server domain axfr -y ns1-ns2.pcX.net :lksdjfq38475-qejflavna==
```

Note: If the time difference between master & slave is more than 3 minutes, the zone transfer will fail even if you have the correct key.