Automated zone signing with BIND

Remember that if you see '#' before a command, it means
you need to run this command as root, either via:

a) sudo -s

b) sudo command

*** ON YOUR MASTER (auth1) SERVER ***

1. First, verify that DNSSEC is enabled in /etc/namedb/named.conf
   In the options { .. }; section, add the following, if it's not
   already there:

   dnssec-enable yes;

   Then find the definition for your zone ("mytld").

   * Note: in a previous lab, you may have modified the definition of your
   zone, so that you were loading the signed version of the zone (.signed) -
   so check if If your zone file configuration is already pointing to
   "mytld.signed", and revert this to "mytld", like in the example below:

```
   zone "mytld" {
     file "/etc/namedb/master/mytld";
     type master;
     allow-transfer { key mydomain-key; };

     key-directory "/etc/namedb/keys";       // <--- Add this
     auto-dnssec maintain;                   // <--- Add this
     update-policy local;                    // <--- Add this
     // dnssec-secure-to-insecure yes;       // <--- Add this
   };
```

    Save and exit

2. If you have made a backup of your zone file, let's copy it back over
   our zone:

```
     # cd /etc/namedb/master
     # cp mytld.backup mytld
```

3. Now reconfig the nameserver

```
    # rndc reconfig
```

      Make sure that your server still answers for your zone, using dig!

```
      # dig @localhost mytld NS
```

    Create a directory for the keys:

```
    # mkdir /etc/namedb/keys
    # chown bind /etc/namedb/keys
```

    Give ownership of the /etc/namedb/master directory so BIND can sign
    your zone and write the file:

```
    # chown -R bind /etc/namedb/master
```

4. Preparing the keys

   If you've done the manual lab from before, you have already
   generated keys, and we can reuse those. Otherwise, we'll generate
   a new set of keys.

a) You already have keys

```
  # cd /etc/namedb/master
  # mv Kmytld* ../keys
```

  ... and skip to step 5

  b) If you don't have keys yet:

```
# cd /etc/namedb/keys
```

  - Generate first key pair (Zone Signing Key)

```
# dnssec-keygen mytld

(  will output something like:
Generating key pair.....................+++++ + ....
Kmytld.+005+43116)
```

  - Generate second key pair (Key Signing Key)

```
# dnssec-keygen -f KSK mytld
Kmytld.+005+52159
```

(once again, some output will show)

  Notice that we don't specify any flags such as algorithm, key size,
  etc... We're using the defaults

5. Let's look at the keys:

```
  # cd /etc/namedb/keys

# ls -l Kmytld*
-rw-r--r--  1 root  wheel   591 Feb 18 15:52 Kmytld.+005+32044.key
-rw-------  1 root  wheel  1774 Feb 18 15:52 Kmytld.+005+32044.private
-rw-r--r--  1 root  wheel   417 Feb 18 15:52 Kmytld.+005+64860.key
-rw-------  1 root  wheel  1010 Feb 18 15:52 Kmytld.+005+64860.private
```

Make the keys readable by BIND:

```
# chgrp bind K*
# chmod g+r K*
```

6. We're ready to sign!

First take a backup of the zone before it was signed

```
    # cd /etc/namedb/master
    # cp mytld mytld.unsigned

      If there is an old "mytld.signed" file, you can get rid of it just in
      case, but it won't be used anyway (this is just to avoid confusion):

      # rm mytld.signed

    Signal BIND to sign the zone (the backup made above will be untouched)

    # rndc sign mytld

    Take a look at the /etc/namedb/log/general log:

    # tail -10 /etc/namedb/log/general

18-Feb-2011 15:57:41.168 set up managed keys zone for view _default, file 'managed-
keys.bind'
18-Feb-2011 15:57:41.184 reloading configuration succeeded
18-Feb-2011 15:57:41.193 any newly configured zones are now loaded
18-Feb-2011 15:57:43.666 received control channel command 'sign mytld'
18-Feb-2011 15:57:43.668 zone mytlf/IN: reconfiguring zone keys
18-Feb-2011 15:57:43.693 zone mytlf/IN: next key event: 19-Feb-2011 03:57:43.693

7. Take a look at the signed zone:

    # cd /etc/namedb/master
    # ls -l mytld*

    Notice the ".jnl" file:

    -rw-r--r--  1 bind  wheel   535 Feb 18 14:22 mytld
    -rw-r--r--  1 bind  wheel  3473 Feb 18 15:57 mytld.jnl

    The zone is now DYNAMICALLY managed by bind.

    If you want to make changes, you either need to:

    a) freeze the zone, edit, thaw:

        # rndc freeze mytld
        # vi ...   // remember the serial!
        # rndc thaw mytld

    b) use nsupdate

        # nsupdate -l
        > update add mail.mytld. 300 A 1.2.3.4
        > send
        > quit

    # tail -10 /etc/namedb/log/general

18-Feb-2011 16:07:00.374 client 127.0.0.1#57195: updating zone 'mytld/IN': adding
an RR at 'mail.phil' A

      If you use the nsupdate method, check the SOA after every update --
      what do you notice ?
```

8. Now we need to include the DS in the parent zone !

   (DS = digest fingerprint of the Key Signing Key).

   Generate a "DS" from your key:

   Find which key is the key signing key:

   ```
   # cd /etc/namedb/keys
   # more Kmytld*key
   ```

   Look at which one has "IN DNSKEY 257". Find the "keyid" and replace the string "+005+32044" below with "+005+keyid" where "keyid" is the number displayed.

   ```
   # dnssec-dsfromkey Kmytld.+005+32044 >dsset-mytld.
   ```

   REMEMBER the dot!

9. Upload the dsset for your zone (containing the hash of your zone) to the ROOT server:

   ```
   # scp dsset-mytld. sysadm@a.root-servers.net:
   ```

   The password is the same as in class

10. Tell the instructor you have done so!

    The instructor will include the DS-set in the root and re-sign the zone