LAB: securing nameserver (DNSSEC)

Lab Environment:

The workshop wifi:

SSID: workshop

PASS: iij/2497

Hosts - Virtual machines (Ubuntu16.04LTS/LXC):

Hostname: nsXX.local

IPv6: fd00:2497:1::X

IPv4: 10.0.0.X

Note: XX is your group id

For group1, it's ns01.local, fd00:2497:1::1 and 10.0.0.1

For group10, its' ns10.local, fd00:2497:1::10 and 10.0.0.10

username: workshop

password: iij/2497

Domain names:

groupXX.local

Note: XX is your gourp id

group01.local for group1, group10.local for group10, and so on

configure DNSSEC with bind9:

ssh to your host, and create 'keys' directrory under /etc/bind to store your dnssec keys (ZSK and KSK). Then generate keys In this example, we use RSASHA256 1024bit for ZSK, and RSASHA256 2048bit for KSK

```
$ sudo mkdir /etc/bind/keys
$ cd /etc/bind/keys
$ sudo dnssec-keygen -r /dev/urandom -a RSASHA256 -b 1024 groupXX.local
$ sudo dnssec-keygen -r /dev/urandom -a RSASHA256 -b 2048 -f ksk groupXX.local
```

Note: In this example, we use /dev/urandom to generate keys quickly. If the quality of keys is your concern, you should use better random source.

Sign your zone with your keys, then you should have your signed zone file as 'groupXX.local.signed'

```
$ cd /etc/bind
$ sudo dnssec-signzone -S  -K keys  groupXX.local
```

Note: By default, the signed zone file is valid for 30 days. That means you need to re-sign your zone file every 30 or less days. Don't forget it.

Edit your zone file configuration to serve with the singed zone.

```
zone "groupXX.local" {
        type master;
        file "/etc/bind/groupXX.local.signed";
};
```

Note: XX is your group id

Let bind9 load the signed zone file.

```
$ sudo  systemctl restart bind9
```

Query your records by dig. You should be able to see RRSIG and DNSKEY records. If not, check your configurations.

```
$ dig  any  groupXX.local  @localhost
```

Register your DS records to the parent zone:

There is 'dsset-groupXX.local.' file in /etc/bind directory on your nsXX host, and this is your DS records to be registered to your parent zone.

$ cat /etc/bind/dsset-groupXX.local.

Copy the file to your web server and make it accessible through the following URL: http://www.groupXX.local/dsset-groupXX.local.

Note: XX is your group id

$ scp /etc/bind/dsset-groupXX.local. workshop@www.groupXX.local:~/

ssh to your web server and copy the file to your web contents directory

$ ssh www.groupXX.local

$ sudo cp ./dsset-groupXX.local. /var/www/html/

Make sure you can access the file through the above URL, and ask instructors to fetch and register it.

Once instructors put your DS records into the parent zone, your zone should be able to validate by DNSSEC. Check those by querying your records, you'll see 'AD' bit on if succeed.

$ dig any groupXX.local

Add and remove some records on your nsXX host, sign the zone file, reload it and check again.

$ cd /etc/bind

$ sudo vi /etc/bind/groupXX.local

$ sudo dnssec-signzone -S -K keys groupXX.local

$ sudo rndc reload

$ dig +dnssec www.groupXX.local