PRACTICAL:

Please Note the practical will be done in groups

Two servers:

primary (your group)

secondary (next group)

- CentOS
- BIND 9
- domain: groupx.co.ke
- Primary IP address: 196.X.X.X
- Secondary IP address: 196.X.X.X

DNSSEC Master Configuration

vi /etc/named.conf

Ensure the following lines are present:

dnssec-enable yes;

dnssec-validation yes;
dnssec-lookaside auto;

Here is the full named.conf file example adjusted for authoritative name services.

```
options {
   listen-on port 53 { any; };
   listen-on-v6 port 53 { any; };
   directory       "/var/named";
   dump-file       "/var/named/data/cache_dump.db";
```

```
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
    allow-transfer  { none; };
    recursion no;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
```

```
    type hint;
    file "named.ca";
};


include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

To install haveged on RHEL/CentOS , you first need to add the EPEL repository by following the instructions

```
su -c 'rpm -Uvh https://download.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm'
su -c 'yum install foo'
```

Once you've installed and enabled the EPEL repo (on RHEL/CentOS), you can install haveged by running the following command:

yum install haveged

make sure it's configured to start at boot:

chkconfig haveged on

Navigate to the location of your zone files:

cd /var/named/

Create a Zone Signing Key(ZSK) with the following command.

dnssec-keygen -a RSASHA256 -b 2048 -n ZONE yourdomain.co.ke

SAMPLE OUTPUT:
Generating key pair.....+++ .....+++
Kyourdomain.co.ke.+007+40400

Create a Key Signing Key(KSK) with the following command:

dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE yourdomain.co.ke

SAMPLE OUTPUT:
Generating key pair.....+
+ .....
.....++
Kyourdomain.co.ke.+007+62910

The directory will now have 4 keys - private/public pairs of ZSK and KSK. We have to add the public keys which contain the **DNSKEY** record to the zone file. The following for loop will do this.

cat Kgroup8*key >>group8.co.ke.zone

Sign the zone with the dnssec-signzone command.

dnssec-signzone -3 <salt> -A -N INCREMENT -o <zonename> -t <zonefilename>

Replace salt with something random. Here is an example with the output.

dnssec-signzone -e +3024000 -o yourdomain.co.ke -N INCREMENT yourdomain.co.ke.zone

A 16 character string must be entered as the "salt"

This creates a new file named yourdomain.co.ke.zone.signed which contains **RRSIG** records for each DNS record. We have to tell BIND to load this "signed" zone.

Zones file is /etc/named.rfc1912.zones

```
vi  /etc/named.rfc1912.zones
```

Change the file option inside the zone { } section.

```
zone "yourdomain.co.ke" IN {
    type master;
    file "yourdomain.co.ke.zone.signed";
    allow-transfer { yourslaveIP; };
    allow-update { none; };
};
```

Save this file and reload bind

Check if for the DNSKEY record using dig on the same server.

```
dig DNSKEY yourdomain.co.ke. @localhost +multiline
```

Output should have:

```
;; ANSWER SECTION:
yourdomain.co.ke.       86400 IN DNSKEY   256 3 7 (
                AwEAActPMYurNEyhUgHjPctbLCI1VuSj3xcjI8QFTpdM
                8k3cYrfwB/WlNKjnnjt98nPmHv6frnuvs2LKIvvGzz++
                kVwVc8uMLVyLOxVeKhygDurFQpLNNdPumuc2MMRvV9me
                fPrdKWtEEtOxq6Pce3DW2qRLjyE1n1oEq44gixn6hjgo
                sG2FzV4fTQdxdYCzlYjsaZwy0Kww4HpIaozGNjoDQVI/
                f3JtLpE1MYEb9DiUVMjkwVR5yH2UhJwZH6VVvDOZg6u6
                YPOSUDVvyofCGcICLqUOG+qITYVucyIWgZtHZUb49dpG
```

```
        aJTAdVKlOTbYV9sbmHNuMuGt+1/rc+StsjTPTHU=
        ) ; key id = 40400
yourdomain.co.ke.       86400 IN DNSKEY   257 3 7 (
        AwEAAa2BE0dAvMs0pe2f+D6HaCyiFSHw47BA82YGs7Sj
        qSqH3MprNra9/4S0aV6SSqHM3iYZt5NRQNTNTRzkE18e
        3j9AGV8JA+xbEow74n0eu33phoxq7rOpd/N1GpCrxUsG
        kK4PDkm+R0hhfufe1ZOSoiZUV7y8OVGFB+cmaVb7sYqB
        RxeWPi1Z6Fj1/5oKwB6Zqbs7s7pmxl/GcjTvdQkMFtOQ
        AFGqaaSxVrisjq7H3nUj4hJIJ+SStZ59qfW3rO7+Eqgo
        1aDYaz+jFHZ+nTc/os4Z51eMWsZPYRnPRJG2EjJmkBrJ
        huZ9x0qnjEjUPAcUgMVqTo3hkRv0D24I10LAVQLETuw/
        QOuWMG1VjybzLbXi5YScwcBDAgtEpsQA9o7u6VC00DGh
        +2+4RmgrQ7mQ5A9MwhglVPaNXKuI6sEGlWripgTwm425
        JFv2tGHROS55Hxx06A416MtxBpSEaPMYUs6jSIyf9cjB
        BMV24OjkCxdz29zi+OyUyHwirW51BFSaOQuzaRiOsovM
        NSEgKWLwzwsQ5cVJBEMw89c2V0sHa4yuI5rr79msRgZT
        KCD7wa1Hyp7s/r+ylHhjpqrZwViOPU7tAGZ3IkkJ2SMI
        e/h+FGiwXXhr769EHbVE/PqvdbpcsgsDqFu0K2oqY70u
        SxnsLB8uVKYlzjG+UIoQzefBluQl
        ) ; key id = 62910

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 27 18:18:30 2013
;; MSG SIZE  rcvd: 839
```

DNSSEC Slave Configuration

The slave servers only require DNSSEC to be enabled and the zone file location to be changed. Edit the main configuration file of BIND.

vi /etc/named.conf
Place these lines inside the options { } section if they don't exist.

```
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
```

Edit the file option inside the zone { } section.

```
zone "yourdomain.co.ke" IN {
   type slave;
   file "yourdomain.co.ke.zone.signed";
   masters { masterIP; };
};
```

Reload the BIND service.

Check if there is a new .signed zone file.

```
[root@slave ~]# ls -l /var/named/slaves/
```

Configure DS records with the registrar

When we ran the dnssec-signzone command apart from the .signed zone file, a file named dsset-yourdomain.co.ke was also created, this contains the DS records.

```
root@master:/var/cache/bind# cat dsset-yourdomain.co.ke.
Yourdomain.co.ke.       IN DS 62910 7 1
1D6AC75083F3CEC31861993E325E0EEC7E97D1DD
yourdomain.co.ke.       IN DS 62910 7 2
198303E265A856DE8FE6330EDB5AA76F3537C10783151AEF3577859F FFC3F59D
```

Add to the registry

**********TAIL END**********

Once this is confirmed, we can check if DNSSEC is working fine using any of the following online services.

- http://dnssec-debugger.verisignlabs.com
- http://dnsviz.net/