Lab 11 - OpenDNSSEC

Objective:
Use OpenDNSSEC to automate key signing.

Background
DNSSEC (or DNS Security Extensions) provide security to the zone files.

Steps:

A. Installing dependencies of OpenDNSSEC

1. Install LDNS, a DNS programming library.

```
./configure –prefix=/usr (–disable-gost)
make
sudo make install
```

2. Install Libxml2

```
./configure; make; make install
```

3. Install MySQL (optional)

4. Install SQLite

```
./configure; make; make install
```

B. Install a Hardware Security Module (HSM)

1. Install SoftHSM and its dependencies.

Dependencies: Botan 1.10.0, OpenSSL 0.9.8

```
tar xvzf softhsm-<version>.tar.gz
cd softhsm-<version>
make
sudo make install
```

2. In /etc/softhsm.conf, add this line:

```
export SOFTHSM_CONF=/home/user/config.file
```

3. Open the config file and specify what slots will be used.

```
vi /home/user/config.file
0:/home/user/my.db
4:/home/user/token.tabels
```

Initialize the tokens. Add a label to your token. Labels must be unique.

```
softhsm-init-token slot 0 –label "opendnssec-KSK"
softhsm-init-token slot 0 –label "opendnssec-ZSK"
```

(type in the SO pin and USER pin)

C. Install and run OpenDNSSEC

1. Install dependencies.
2. Install OpenDNSSEC

```
yum –y install opendnssec
```

Or from source

```
wget http://opendnssec.org/path/to/opendnssec-version.tar.gz
tar xzvf opendnssec-version
cd opendnssec-version
make
sudo make install
```

3. Rebuild the dynamic linker.

```
sudo ldconfig
```

4. Initialize and create database.

```
ods-ksmutil setup
```

5. Start the two daemons using

```
ods-control start
```

D. Configuring OpenDNSSEC XML Files

1. Main Configuration – CONF.XML

   All configuration files are stored in /etc/opendnssec/ folder by default. Open conf.xml.

sudo vi /etc/opendnssec/conf.xml

These are the configuration options you need to modify:

RepositoryList- defines the HSM

Common – common configuration

Enforcer – the part that constructs the signature records

Add the repository in conf.xml and point to the HSM. Keep in mind that the TokenLabel should match with the label used in SoftHSM.

```
<Repository name="SoftHSM">
<Module>/usr/local/lib/libsofthsm.so</Module>
<TokenLabel>OpenDNSSEC-KSK</TokenLabel>
 <PIN>1234</PIN>
 </Repository>
```

Add or uncomment the common directive, and point to the direction of your KASP and ZONELIST XML files.

```
<Common>
<Logging>
<Syslog><Facility>local0</Facility></Syslog>
</Logging>
<PolicyFile>/etc/opendnssec/kasp.xml</PolicyFile>
<ZoneListFile>/etc/opendnssec/zonelist.xml</ZoneListFile>
<!--
<ZoneFetchFile>/etc/opendnssec/zonefetch.xml</ZoneFetchFile>
-->
</Common>
```

The Enforcer points to the SQL database and provides info on the user who can use it.

```
<Enforcer>
<Privileges>
<User>ods</User>
<Group>ods</Group>
</Privileges>
<Datastore><SQLite>/var/opendnssec/kasp.db</SQLite></Datastore>
<Interval>PT3600S</Interval>
</Enforcer>
```

The signer points to a temporary directory, which will be used to store files during the signing process.

```
<Signer>
<Privileges>
<User>ods</User>
<Group>ods</Group>
</Privileges>
<WorkingDirectory>/var/opendnssec/tmp</WorkingDirectory>
<WorkerThreads>4</WorkerThreads></Signer>
```

2. Key and Signature Policy – KASP.XML

   Create your custom policy and name it accordingly:

```
<Policy name = "Net-A-policy">
            <Description>Create a descriptive comment
here</Description>
</Policy>
```

   In the Signature directive, provide timing parameters used by the signing engine.

   - Resign – interval between runs of the Signer engine
   - Refresh – when a signature should be refreshed
   - Validity – how long the signatures are valid for. Set to default for all RRSIGs and Deny for NSEC/NSEC3
   - Jitter – ensure that not all signature expires at the same time

   The Denial directive provides NSEC/NSEC3 info – which algorithm to use and the salt length.

   The Keys directive provides parameters that are common for both KSK and ZSK. Parameters specifically for one key should be within its own directive, i.e. KSK directive for KSK options.

3. Zone list – ZONELIST.XML

   The zonelist shows the zones to be signed. It points three important files:

   - specific Signer configuration for that zone
   - Input adapters - the unsigned zonefile
   - Output adapters – where to store the signed zonefile

E. Adding Zones

1. To add zones, use the command below. Or add manually by editing zonelist.xml

```
ods-ksmutil zone add --zone <zonename>
```

2. Afterward, execute the following command:

```
ods-ksmutil update zone list
```

F. Troubleshooting

1. To check if the config files are valid

```
ods-kaspcheck
```

2. Error logging is done via the system's syslog facility. Edit the file /etc/rsyslog.conf

```
<logging>
<syslog><facility>local0</facility></syslog>
</logging>
```